

COMMUNICATION METHOD, COMMUNICATION SYSTEM, USER TERMINAL AND COMMUNICATION CONNECTION PROGRAM

Publication number: JP2003060675

Publication date: 2003-02-28

Inventor: KITADA ATSUSHI; OKUDA MASAHIITO

Applicant: FUJITSU LTD

Classification:

- international: H04L12/46; H04L29/06; H04L29/12; H04L29/08;
H04L12/46; H04L29/06; H04L29/12; H04L29/08; (IPC1-
7): H04L12/56; H04L12/46; H04L29/08

- european: H04L12/46V; H04L29/06; H04L29/06C6C2; H04L29/12A

Application number: JP20010246400 20010815

Priority number(s): JP20010246400 20010815

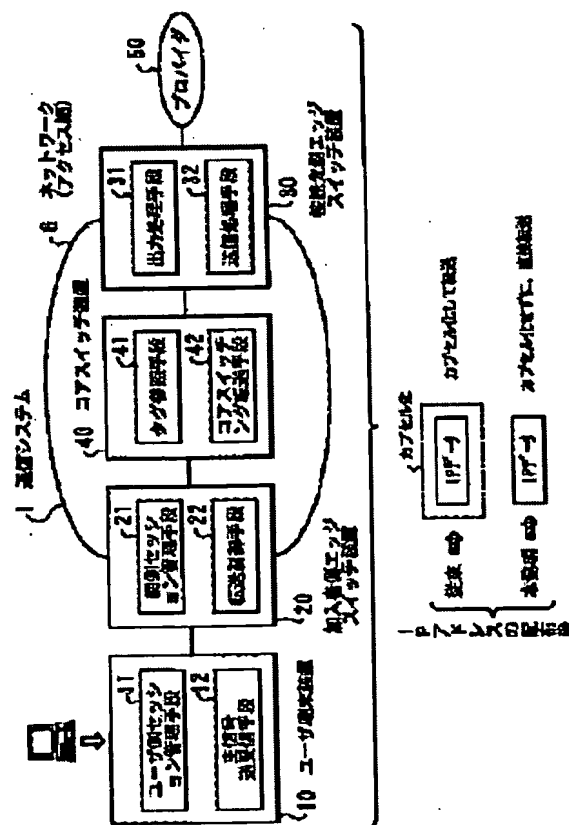
Also published as:

US2003037163 (A)

Report a data error here

Abstract of JP2003060675

PROBLEM TO BE SOLVED: To construct a high speed communication system to realize an efficient destination party switching, thereby improving the quality of the communication service. **SOLUTION:** A user side session control means 11 controls the designation of a destination address, user authentication and IP address allotment at an authentication phase. A main signal transmitting/receiving means 12 transmits/ receives not capsulated main signal frames at a communication phase. A network side session control means 21 performs the signaling control. A transfer control means 22 transfers main signal frames with a tag added for univocally showing a virtual closed network, upon receipt of the signal frames from a user and also transfers main signal frames to a user terminal 10, without the tag, upon receipt thereof from a destination party. An output processing means 31 outputs the main signal frames, without the tag, to the destination party, as the tag corresponds to its output port. A transmission processing means 32 determines the designation party from an input port and transmits a signal with an added tag to the user terminal 10.



Data supplied from the esp@cenet database - Worldwide

BEST AVAILABLE COPY

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-60675

(P2003-60675A)

(43) 公開日 平成15年2月28日 (2003.2.28)

(51)Int.Cl. ⁷	識別記号	F I	テーマコード [*] (参考)
H 0 4 L	12/56	H 0 4 L	H 5 K 0 3 0
	12/46		V 5 K 0 3 3
	29/08		3 0 7 A 5 K 0 3 4

審査請求 未請求 請求項の数10 O L (全 43 頁)

(21) 出願番号 特願2001-246400 (P2001-246400)

(22) 出願日 平成13年8月15日 (2001.8.15)

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番
1号

(72) 発明者 北田 敦史

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(72) 発明者 奥田 将人

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(74) 代理人 100092152

弁理士 服部 毅蔵

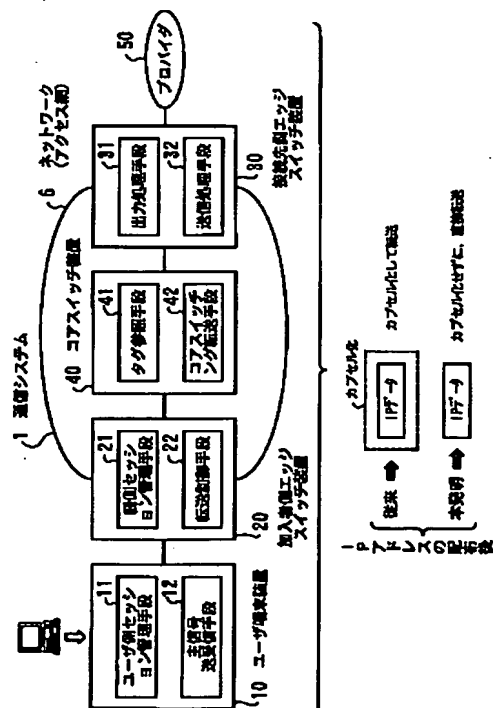
最終頁に続く

(54) 【発明の名称】 通信方法、通信システム、ユーザ端末装置及び通信接続プログラム

(57) 【要約】

【課題】 高速通信可能なシステムを構築して、効率のよい接続先切り替えを実現し、通信サービスの品質の向上を図る。

【解決手段】 ユーザ側セッション管理手段11は、認証フェーズ時に、制御フレームを用いて、接続先の指定、ユーザ認証及びIPアドレス割り当ての制御を行う。主信号送受信手段12は、通信フェーズ時に、カプセル化しない主信号フレームを送受信する。網側セッション管理手段21は、シグナリング制御を行う。転送制御手段22は、ユーザからの主信号フレームの受信時には、仮想閉域網を一意に示すタグを付加して転送し、接続先からの受信時には、タグを外してユーザ端末装置10側へ転送する。出力処理手段31は、タグと出力ポートとが対応して、タグを外して接続先へ主信号フレームを出力する。送信処理手段32は、入力ポートより接続先を判断し、タグを付加してユーザ端末装置10側へ送信する。



【特許請求の範囲】

【請求項1】 ユーザからは、IPoEで主信号フレームを送受信し、

前記ユーザでは、レイヤ2レベルで前記主信号フレームと区別可能な制御フレームによって、接続先の指定、ユーザ認証及びIPアドレス割り当ての処理を含む制御を行い、

アクセス網にとっては、接続先仮想閉域網を識別して、送信元MACアドレスと、前記接続先仮想閉域網とをマッピングし、

前記アクセス網では、MACブリッジングによってレイヤ2レベルの転送を行うことを特徴とする通信方法。

【請求項2】 アクセス網と、

認証フェーズ時に、制御フレームを用いて、接続先の指定、ユーザ認証及びIPアドレス割り当ての処理を含む制御を行うユーザ側セッション管理手段と、通信フェーズ時に、カプセル化しない主信号フレームを送受信する主信号送受信手段と、から構成されて仮想閉域網に対するレイヤ2での接続を行うユーザ端末装置と、を有することを特徴とする通信システム。

【請求項3】 前記制御フレームの受信時には、シグナリング制御を行う網側セッション管理手段と、ユーザから転送された主信号フレームの受信時には、仮想閉域網を一意に示すタグを付加して転送し、前記接続先から転送された主信号フレームの受信時には、前記タグを外して前記ユーザ端末装置側へ転送する転送制御手段と、から構成される加入者側エッジスイッチ装置をさらに有することを特徴とする請求項2記載の通信システム。

【請求項4】 複数の前記接続先と同時接続する場合、前記転送制御手段は、前記ユーザ端末装置及び前記接続先それぞれのレイヤ2アドレスにより、接続先を一意に識別することを特徴とする請求項3記載の通信システム。

【請求項5】 前記タグと出力ポートとが対応して、前記タグを外して前記接続先へ主信号フレームを出力する出力処理手段と、入力ポートより前記接続先を判断し、前記タグを付加して前記ユーザ端末装置側へ送信する送信処理手段と、から構成される接続先側エッジスイッチ装置をさらに有することを特徴とする請求項2記載の通信システム。

【請求項6】 前記加入者側エッジスイッチ装置及び前記接続先側エッジスイッチ装置は、レイヤ2アドレスとレイヤ3アドレスの対応を示すテーブルを生成し、送信元装置から宛先装置のレイヤ2アドレスを求めるリクエストがあった場合、前記テーブルにもとづき、前記宛先装置の代理応答を行って、前記レイヤ2アドレスを返信して、アドレス解決制御を行うアドレス解決手段をさらに有することを特徴とする請求項2記載の通信システム。

【請求項7】 前記ユーザ端末装置からの認証情報の集

約、前記認証情報の前記接続先への転送、前記接続先で認証制御された結果を示す認証メッセージの前記ユーザ端末装置への転送、を含む認証に関する一元管理処理を行う通信管理サーバをさらに有することを特徴とする請求項2記載の通信システム。

【請求項8】 前記網側セッション管理手段を前記通信管理サーバに、前記転送制御手段を前記加入者側エッジスイッチ装置に持たせて、前記制御フレームの処理と、前記主信号フレームの処理とを装置的に分離することを特徴とする請求項7記載の通信システム。

【請求項9】 認証フェーズ時に、制御フレームを用いて、接続先の指定、ユーザ認証及びIPアドレス割り当ての処理を含む制御を行うユーザ側セッション管理手段と、

通信フェーズ時に、カプセル化しない主信号フレームを送受信する主信号送受信手段と、

を有することを特徴とする、仮想閉域網に対するレイヤ2での接続を行うユーザ端末装置。

【請求項10】 ユーザ端末装置側に装備され、仮想閉域網に対するレイヤ2での接続を行う通信接続プログラムにおいて、

コンピュータに、

認証フェーズ時に、制御フレームを用いて、接続先の指定、ユーザ認証及びIPアドレス割り当ての処理を含む制御を行い、

通信フェーズ時に、カプセル化しない主信号フレームを送受信する、

処理を実行させることを特徴とする通信接続プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、通信方法、通信システム、ユーザ端末装置及び通信接続プログラムに関し、特にユーザとプロバイダ間の通信サービス実行時の通信制御を行う通信方法、ユーザとプロバイダ間の通信サービス実行時の通信制御を行う通信システム、仮想閉域網に対するレイヤ2での接続を行うユーザ端末装置及びユーザ端末装置側に装備され、仮想閉域網に対するレイヤ2での接続を行う通信接続プログラムに関する。

【0002】

【従来の技術】インターネット、デジタルコンテンツ配信など広帯域マルチメディアサービスの普及に伴い、ネットワークの経済的で高速・広帯域なシステムの開発が急速に進められている。

【0003】例えば、既設の電話用銅線ケーブルを利用して、高速なデジタル伝送を行うADSL(Asymmetric Digital Subscriber Line)や、ユーザ宅に光ファイバケーブルを敷設して、ユーザ端末からより高速・大容量の通信サービスを実現するFTTH(Fiber To The Home)などのシステム構築が進められている。

【0004】また、このようなネットワーク技術の発展に伴って、高画質の映像配信サービスや音楽ダウンロードサービスなどを提供するxSP(インターネット・サービス・プロバイダやコンテンツ・サービス・プロバイダ等)が、数多く出現すると考えられ、ネットワーク・ビジネス市場の拡大に拍車をかけている。

【0005】また、近年ではVPN(Virtual Private Network: 仮想閉域網)と呼ばれるネットワーク・サービスが提供されている。これは、社内で構築したネットワークを使って、通信事業者のサービスを、あたかも専用線のように利用できるサービスの総称である。

【0006】このVPNにより、例えば、社内のLANをインターネット経由で接続して、仮想的にプライベート・ネットワークを構築することにより、物理的なネットワーク構成に縛られることのない、柔軟で拡張性のあるネットワークを構築することができる。

【0007】このように、現在のブロードバンド・サービスが広がりつつある状況の中で、ユーザ側では、接続先であるプロバイダを、用途に応じてより柔軟に切り替えたいという要求が高まってきている。

【0008】一方、LANの技術であるイーサネット(Ethernet)(登録商標)がアクセス回線やWAN回線のテクノロジーとして有望視されている(10Gb/sへの標準化等)。そこで、接続先切り替え機能に必須な、認証/IPアドレス割り当てをイーサネット上で行う方式として、PPPoE(Point-to-Point Protocol over Ethernet)がある。

【0009】図65はユーザとプロバイダとの接続形態を示す図である。図は、PPPoEを利用して、プロバイダへの接続先が切り替え可能な接続形態を示している。イーサネット上のユーザ端末100は、加入者側の終端装置110として、サービス形式がADSLならばADSLモデムに接続し、FTTHならばONU(Optical Network Unit)に接続する。ADSLモデムやONUは、ADSL回線またはFTTHの光回線を通じ、アクセス網600を介してプロバイダに接続する。

【0010】ユーザからプロバイダへ接続する際には、ユーザ端末100は、まず、プロバイダへ発呼し、ユーザIDとパスワードを送信する。そして、プロバイダ側で認証されると、IPアドレスが配布されて、その後サービスが開始される。また、接続先の変更は、ユーザIDの後に、変更したいプロバイダ名を続けて打ち込んで送信することで、網側がこれを識別して接続先を切り替える。

【0011】なお、発呼後の一連の処理は、PPPで実行されるため、IPアドレスの配布には、IPCP(Internet Protocol Control Protocol)が用いられる。ここで、PPPのレイヤは、LCP(Link Control Protocol)とNCP(Network Control Protocol)の2階層で構成される。LCPは、上位プロトコルに依存しない

データリンクの確立を実現し、NCPは、上位プロトコルに依存した処理を受け持つものである。そして、上位プロトコルがTCP/IPの場合には、NCPとしてはIPCPが用いられ、IPCPによりIPアドレスの決定処理が行われる。

【0012】図66はPPPoEを利用した従来のネットワークシステムを示す図である。図65で上述した内容を、ネットワークシステム全体で示した際の概略図である。ユーザ端末100は、アクセス網600に接続する(終端装置の図示は省略)。アクセス網600にはスイッチ部601、B-RAS(Broadband Remote Access Server)610が設置され、B-RAS610は、プロバイダ側のサーバに接続する。

【0013】このようなシステムに対して、ユーザからプロバイダへ接続する場合、ユーザ端末100では「ユーザ名@プロバイダ名」と指定し、この情報はスイッチ部601を介して、B-RAS610へ送信される。B-RAS610ではこの情報にもとづいて、接続先のプロバイダに対して、受信したユーザパケットを振り分ける。このような処理によって、ユーザは接続先を任意に選択する。

【0014】

【発明が解決しようとする課題】しかし、上記のようなPPPoEを用いた従来のネットワークシステムでは、B-RAS610に処理が集中してしまうために、処理負荷が非常に重く、高速通信アクセス実現の妨げになるといった問題があった。

【0015】B-RAS610に処理が集中する理由としては、例えば、IP処理をしなければならないため、各xSPへ接続されるインタフェース毎にIPアドレスを設定しなければならない、またユーザとPoint-to-Point接続を行うPPP仮想インタフェースにもIPアドレスが割り振られるため、管理工数がかかってしまうといったことや、異なるxSPに接続する際に、同じユーザなのにセッション管理を行うB-RASが異なっていると、統計情報や課金などの管理工数がかかってしまうなどといった理由が挙げられる。

【0016】また、図66に示したように、ユーザ端末100からのフレームは、どのプロバイダと接続する場合でも、B-RAS610を経由する。そして、PPPoEでは、認証などの制御情報だけでなく、IPパケットなどユーザデータもPPPでカプセル化して転送している。したがって、B-RAS610は、すべてのユーザの制御情報だけでなく、プロバイダに転送する主信号までもが集中してしまう。

【0017】PPPoEにおける制御情報のネゴシエーションは、互いに条件をリクエスト(Configure-Request)し合って、互いに承認(Configure-Ack)しあう必要がある。しかも、ユーザ毎に条件が異なるため、ソフトウェア処理が前提となる。

【0018】また、プロバイダに転送するためには、B-RAS610は、レイヤ3の処理もしなければならず（仮想ルータ機能と呼ばれる）、全インタフェース分（プロバイダ数×加入者数だけのPPP仮想インタフェース及びプロバイダ側インタフェース）のルーティングテーブルをハンドリングする必要がある。

【0019】このように、従来では上記のような多岐にわたる処理を、B-RAS610がすべて行っていたために、B-RAS610がボトルネックとなっており、PPPoEを利用した従来のネットワークシステムでは高速化に限界があった。

【0020】本発明はこのような点に鑑みてなされたものであり、高速通信可能なシステムを構築して、効率のよい接続先切り替えを実現し、ユーザとプロバイダ間での通信サービスの品質の向上を図った通信方法及び通信システムを提供することを目的とする。

【0021】また、本発明の他の目的は、効率のよい接続先切り替えを実現し、通信サービスの品質の向上を図ったユーザ端末装置を提供することである。さらに、本発明の他の目的は、効率のよい接続先切り替えを実現し、通信サービスの品質の向上を図った通信接続プログラムを提供することである。

【0022】

【課題を解決するための手段】本発明では上記課題を解決するために、図1に示すような、本発明の通信方法をもとに構成された通信システム1において、アクセス網6と、認証フェーズ時に、制御フレームを用いて、接続先の指定、ユーザ認証及びIPアドレス割り当ての処理を含む制御を行うユーザ側セッション管理手段11と、通信フェーズ時に、カプセル化しない主信号フレームを送受信する主信号送受信手段12と、から構成されてレイヤ2での通信接続を行うユーザ端末装置10と、制御フレームの受信時には、シグナリング制御を行う網側セッション管理手段21と、ユーザから転送された主信号フレームの受信時には、仮想閉域網を一意に示すタグを付加して転送し、接続先から転送された主信号フレームの受信時には、タグを外してユーザ端末装置10側へ転送する転送制御手段22と、から構成される加入者側エッジスイッチ装置20と、タグと出力ポートとが対応して、タグを外して接続先へ主信号フレームを出力する出力処理手段31と、入力ポートより接続先を判断し、タグを付加してユーザ端末装置10側へ送信する送信処理手段32と、から構成される接続先側エッジスイッチ装置30と、を有することを特徴とする通信システム1が提供される。

【0023】ここで、ユーザ側セッション管理手段11は、認証フェーズ時に、制御フレームを用いて、接続先の指定、ユーザ認証及びIPアドレス割り当ての処理を含む制御を行う。主信号送受信手段12は、通信フェーズ時に、カプセル化しない主信号フレームを送受信す

る。網側セッション管理手段21は、制御フレームの受信時には、シグナリング制御を行う。転送制御手段22は、ユーザから転送された主信号フレームの受信時には、仮想閉域網を一意に示すタグを付加して転送し、接続先から転送された主信号フレームの受信時には、タグを外してユーザ端末装置10側へ転送する。出力処理手段31は、タグと出力ポートとが対応して、タグを外して接続先へ主信号フレームを出力する。送信処理手段32は、入力ポートより接続先を判断し、タグを付加してユーザ端末装置10側へ送信する。

【0024】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。図1は本発明の通信システムの原理図である。本発明の通信方法をもとに構成された通信システム1は、アクセス網6を通じて、ユーザとプロバイダ間の通信サービス実行時の通信制御を行う。

【0025】ユーザ端末装置10に対し、ユーザ側セッション管理手段11は、認証フェーズ時に、制御フレームを用いて、接続先（xSP：プロバイダ50）の指定及びユーザ認証／IPアドレス割り当ての処理を含む制御を行う。

【0026】主信号送受信手段12は、通信フェーズ（IP通信フェーズ）時に、認証フェーズのプロトコルを介さずに、カプセル化しない主信号フレームを直接（レイヤ2で）送受信する。

【0027】ここで、従来では、ユーザ側の端末が、VPNサービスを利用して、接続先と通信する場合には、認証からIPパケットの送受信までの通信シーケンスをすべてトンネリング・プロトコル（IPパケットに、新しいオーバーバイトヘッダを付加してカプセル化し、相手先に送信するプロトコル）を用いて通信制御していた。

【0028】一方、本発明のユーザ端末装置10では、通信接続シーケンスを、認証フェーズとIP通信フェーズの2つに分け、認証フェーズではPPPoEのプロトコルを使用し、通信フェーズではIP over Ethernet（IPoE）を使用してIPパケットに対するカプセル化はせずに、IPパケットの送受信を行うものである。

【0029】加入者側エッジスイッチ装置20に対し、網側セッション管理手段21は、制御フレームの受信時に、シグナリング制御を行う。転送制御手段22は、ユーザから転送された主信号フレームの受信時には、仮想閉域網を一意に示すタグを付加して転送し、接続先から転送された主信号フレームの受信時には、タグを外してユーザ端末装置10側へ転送する。

【0030】接続先側エッジスイッチ装置30に対し、出力処理手段31は、タグと出力ポートとが対応して、接続先へ主信号フレームを出力する（実際には、xSP側に割り当てていたポートがアクセス網6側のポートとして動作させたり、その逆の動作を行うようなことも可能）。送信処理手段32は、入力ポートより接続先を判

断し、タグを付加してアクセス網6を通じて、ユーザ端末装置10側へ送信する。

【0031】コアシッチ装置40に対し、タグ参照手段41は、受信した主信号フレームのタグを参照する。コアシッチング転送手段42は、レイヤ2レベルで主信号フレームの転送を行う。

【0032】次にPPPoEの従来のVPNシステムに対して、本発明の通信システム1を適用した場合の具体的な構成及び動作について以降詳しく説明する。まず、通信システム1全体の概要について説明する。

【0033】上述したように、PPPではユーザ認証及びIPアドレスの割り当てを受けて、実際のIPデータ通信を行う。このユーザ認証とIPアドレス割当の機構は、xSP切替接続には必須の機能である。ユーザ認証は当然として、xSPを切り替えるということはIPサブネットが切り替わるということであり、IPv6に移行してもサブネットIDの割当を受けることは必須である。しかし、IPアドレス割当後、IPデータに関しては、中継アクセス網において、ユーザが正しく認証されていることを確認して、適切に該当xSPに転送することができれば、PPPでカプセル化して転送する必要性はない。

【0034】したがって、本発明では、PPPoEをシグナリングのメカニズムとしてのみとらえ、IPデータに関しては、カプセル化しない主信号を、IP over Ethernet (IPOE) で直接送受信するようにする。

【0035】すなわち、ユーザがプロバイダと通信する際には、認証フェーズとIP通信フェーズに分けて、各フェーズに対して、レイヤ2レベルで、制御フレームと主信号フレームで認識・処理する。

【0036】したがって、制御フレーム (PPPoE) により、ユーザ端末装置10が発呼して、ユーザ認証及びIPアドレス割当のネゴシエーションを行った後 (認証フェーズ)、ユーザ端末装置10からは、割当を受けたIPアドレスを設定して、主信号フレームであるIPデータ (IPOE) を送出する (IP通信フェーズ)。

【0037】ただし、ユーザ端末装置10と、アクセス網6 (加入者側エッジスイッチ装置20) との接続セッションの維持は、PPPoEのメカニズムを用い、例えば、接続確認 (LCP: Echo-Request/Reply) や切断処理 (LCP: Terminate-Request/Ack) 等は、PPPoEで送受のやりとりを行う。

【0038】そして、アクセス網6での、ユーザのセッション管理については、本発明では、ユーザ端末装置10が接続された、アクセス網6内の加入者側エッジスイッチ装置20において、送信元MAC (Media Access Control) アドレスでユーザのセッションを管理する (なぜなら、制御フレームであるPPPoEフレームも、主信号フレームであるIPOEフレームも、出力するEthernet インタフェースが同じであれば、レイヤ2アドレ

スである送信元MACアドレスは同一であるから)。

【0039】また、加入者側エッジスイッチ装置20は、認証フェーズ完了 (認証成功及びIPアドレス割当完了) 後に、認証フェーズ時に受信した「ユーザ名@プロバイダ名」から抽出した接続先のプロバイダと、送信元MACアドレス (ユーザ端末装置10のMACアドレス) とをマッピングしておく。これにより、送信元MACアドレスから接続先プロバイダを認識して、主信号フレームを転送することが可能になる (MACアドレスでセッションを識別するので、エッジスイッチ装置のポートに複数端末が接続された環境でも適切にセッションを管理できる)。

【0040】なお、ここでの制御はVLAN (Virtual LAN) 技術を応用したものである。VLANとは、入力フレームの伝達範囲を物理的な構成に制限されずに、論理的なネットワークとして構成する技術である。このVLAN機能を用いることで、入力フレームのグループを識別して、同一グループに属する端末にのみフレームを送信することができる。

【0041】また、VLANによる識別制御にはいくつかの種類があり、ここでは、入力フレームの送信元MACアドレスから相手を識別する、MACアドレスVLANを適用している (ただし、従来のMACアドレスVLANは、ユーザのMACアドレスを静的に登録しておくが、本発明では、認証フェーズで抽出した接続先プロバイダに対応して、後述のテーブル登録により、MACアドレスとVLANとの対応を動的に切り替え可能とするものである)。

【0042】一方、加入者側エッジスイッチ装置20では、主信号フレーム (IPOEフレーム) に関して、プロバイダに対応したタグを付加して、アクセス網6を転送する。そして、アクセス網6内のコアシッチ装置40では、タグを参照して、接続先プロバイダを一意に識別し (タグ参照手段)、レイヤ3を見ることなく、レイヤ2レベルのMACブリッジング転送により、主信号フレームの転送を行う (コアシッチング転送手段)。

【0043】なお、本発明では、プロバイダを一意に識別するタグとしてIEEE802.1QのVLAN-Tag (VLAN技術の1つで、4バイトのVLAN-Tagを付加して、このVLAN-Tagからグループ (相手端末) を識別する機能) を用いるが、アクセス網6内でプロバイダを一意に識別できるタグであれば、独自に規定したタグを用いても構わない。

【0044】このように、本発明ではユーザ端末装置10と、加入者側エッジスイッチ装置20とで、シグナリング処理を行い、主信号はIPデータのPPPのカプセル化をせずに、アクセス網6内をレイヤ2レベルで、タグを用いたスイッチングで転送する構成にした。

【0045】これにより、システム内で分散処理が行われるので、従来のような処理負荷が集中するB-RAS

610が不要となり、より柔軟で拡張性に富んだネットワークを構築でき、通信サービスの品質向上を図ることが可能になる。

【0046】また、本発明の効果として、B-RASのかわりに、エッジスイッチ装置に処理を持たせることにしたので、安価にシステムを構築することができる（すなわち、レイヤ3処理を行うルータのような機器に比べ、安価なL2SW (EtherSW) に拡張機能として本発明の機能を設置させることができるので安価に実現可能）。

【0047】さらに、レイヤ2レベルのMACブリッジングで転送するため、アドレス学習は自動で行われ、管理工数の削減を図ることが可能になる（各インタフェース毎にIPアドレスの設定も不要）。また、ユーザのセッション管理は、異なるxSP接続の場合でも、加入者側エッジスイッチ装置（または、後述の通信管理サーバ）で行うことができる。

【0048】なお、加入者側エッジL2SWの加入者側1ポートあたり1ユーザしか接続しない構成であれば、必ずしも（動的）MACアドレスVLANである必要はなく、（動的）ポートVLAN、すなわち認証フェーズ完了後に入力ポートと接続先仮想閉域網をマッピングする方式でも構わない。

【0049】次に本発明を適用した際の他の効果として、IPフラグメント処理を不要とできる旨について説明する。まず、IPoEのIPパケットの最大長（MTU: Maximum Transfer Unit）は1500バイトである。一方、従来のPPPoEでは、IPパケットをPPPでカプセル化して転送するため、8バイトのオーバーヘッドが生じる。したがって、この8バイトのオーバーヘッド分、IPパケット部分が短くなるので、PPPoEのIPパケットのMTUは、1492バイトとなる。

【0050】ここで、従来、ユーザからの上り通信の場合では、LCPでIPパケットのMTUを1492バイトとしてネゴシエーションしているために、フラグメント処理は回避されていた。

【0051】ところが、網側からの下りフレーム（インターネット等からの下りフレーム）は、EthernetでのMTUである1500バイトで送られてくる場合があり、この場合には、B-RAS610やプロバイダ側のルータでは、PPPoEのカプセル化を実行するために、IPのフラグメント処理を施す必要があった。

【0052】フラグメント処理は、一般に負荷の重い処理である。このため、通常の通信制御でも高負荷であったB-RAS610に対し、さらにフラグメント処理が加わってしまうと、さらに効率が低下してしまうことになる（なお、フラグメント禁止フラグがセットされたりすると、フラグメントできないIPパケットは、廃棄されてしまうため、通信の信頼性の低下を引き起こすことになる）。

【0053】図2はフレーム構成を示す図である。

（A）は改正前、（B）は改正後、（C）はPPPoEでカプセル化した場合のフレーム構成を示している。

（A）のフレームは、IEEE802.3委員会での改正前のIPデータフレームの構成である。ヘッダが14バイト、IPパケットのMTUは1500バイト、FCS（フレームチェックシーケンス）は4バイトであり、改正前の最大フレーム長は1518バイトであった。

【0054】（B）のフレームは、IEEE802.3委員会での改正後のIPデータフレームであり、（A）のヘッダ部分が4バイト伸びて、最大フレーム長が改正前の1518バイトから1522バイトに改正されている（IEEE802.3ac-1998）。なお、（B）のフレームは、タグを付加した際の本発明の主信号フレームの構成を表している。

【0055】すなわち、（B）のフレームは、ヘッダ14バイト、IEEE802.1Qで規定されたVLAN-Tagが4バイト、IPパケットのMTUは1500バイト、FCSは4バイトで構成され、最大フレーム長は1522バイトである。

【0056】このように、改正後では、IPパケットのMTUが1500バイトのままで、4バイトのタグを付加できる。このため、本発明に対しては、フラグメント処理は発生しない。

【0057】一方、（C）のフレームは、改正後のフレームをPPPoEでカプセル化した場合を示している。図に示すように、PPPoEでカプセル化する場合、改正後でフレーム長が伸びた場合でも、8バイトのオーバーヘッド部分は、ペイロードに含まれることになるので、IPパケットのMTUは、1492バイトで変わりはない。したがって、PPPoEで通信を行えば、フラグメント処理が発生してしまう可能性がある。

【0058】以上説明したように、本発明では、主信号フレームのMTUサイズは、IPoEの1500バイトで送受信することができるので、フラグメント処理は発生せず、効率のよい通信制御を行うことが可能になる。

【0059】次に通信システム1の具体的な構成について説明する。図3は通信システム1の構成例を示す図である。アクセス網6のユーザ側のエッジ部分には、加入者側エッジスイッチ装置（以下、加入者側エッジL2SW (layer2 switch)）20-1、20-2が配置され、接続先であるプロバイダ側のエッジ部分には、接続先側エッジスイッチ装置（以下、プロバイダ側エッジL2SW）30-1、30-2が配置される。また、アクセス網6内部には、コアスイッチ装置（以下、コアL2SW）40-1、40-2とProxy Radiusサーバ（通信管理サーバに該当）61が配置されて、図のように接続されている。

【0060】また、ユーザ端末装置10-1、10-2は、加入者側エッジL2SW20-1に接続し、ユーザ端末装置10-3は、加入者側エッジL2SW20-2

に接続する。プロバイダ側エッジL2SW30-1、30-2は、それぞれのISPが有するプロバイダエッジルータ51-1、51-2に接続し、プロバイダエッジルータ51-1、51-2にはプロバイダRadiusサーバ52-1、52-2がそれぞれ接続する。

【0061】なお、Radius (Remote Authentication Dial-in User Service) とは、認証機構をネットワークに導入する際に用いられる代表的なプロトコルのことであり (RFC2865で規定されている)、このRadius機能を含むサーバやクライアントをRadiusサーバ、Radiusクライアントと呼ぶ。

【0062】図4は主信号フレームのフォーマットを示す図である。認証フェーズ完了後、ユーザ端末装置10から送信される主信号フレームのフォーマットを示している。

【0063】図2の(B)に対応させると、14バイトのEtherヘッダの部分がDESTINATIONADDR (6バイト)、SOURCE ADDR (6バイト)、ETHER TYPE (2バイト) に該当する。そして、その他のフィールドは、IPパケットに含まれる。

【0064】また、ETHER TYPEはフレームタイプを示すものであり、0x0800ならば、このフレームは主信号フレームであることを示し、0x8863 (PPPoE Discovery Stage用フレーム) または0x8864 (PPPoE Session Stage用フレーム) ならば制御フレームであることを示す。

【0065】認証フェーズ完了後、このような主信号フレームを加入者側エッジL2SW20が受信すると、送信元MACアドレス (上述のSOURCE ADDR) から接続先のプロバイダを識別し、加入者側エッジL2SW20はタグを付加して転送する。なお、受信した送信元MACアドレスがマッピングされていなければ、そのユーザからのフレームは廃棄する。これにより、認証が行われていないユーザからの不正アクセスなどは回避できる。

【0066】図5は主信号フレームのフォーマットを示す図である。タグが付加されたときの主信号フレームのフォーマットを示している。図2の(B)に対応させると、14バイトのEtherヘッダの部分がDESTINATION ADDR (6バイト)、SOURCE ADDR (6バイト)、ETHER TYPE (2バイト) に該当し、4バイトのIEEE802.1QのVLAN-Tagの部分が、TPID (2バイト)、PRI (3ビット)、CFI (1ビット)、VID (12ビット) に該当する。また、ETHER TYPEが0x0800で、TPIDが0x8100のとき、タグ付き主信号フレームであることを示し、VIDフィールドから識別する。

【0067】ここで、タグが付加された主信号フレームは、アクセス網6内のコアL2SW40でスイッチングされて、プロバイダ側エッジL2SW30まで転送されると、プロバイダ側エッジL2SW30でタグが外されて、指定のプロバイダへ到着することになる。逆に、プ

ロバイダからユーザへの下りフレームは、ポートベースのVLANにより (すなわち、プロバイダ側エッジL2SW30のポートに対応してVIDのタグを設定している。後述する。)、上りのときと同様にタグを付加して、アクセス網6内を転送する。

【0068】このように、本発明では、IPパケットをレイヤ2レベルでセキュアに (安全に) プロバイダへ転送することが可能である。そして、レイヤ2レベルで転送することのメリットとしては、将来IPv6に移行した場合にも、レイヤ3を見ることなく、ETHER TYPEで主信号であることを判別して転送可能なため、アクセス網6内の装置を変更する必要がない。なお、IPv6のETHER TYPEは、0x86DDである。

【0069】また、本発明の通信システム1の効果として、図3のような構成にすることにより、既存設備をほとんど変更なく流用可能な点を挙げることができる。図3に示す構成に対し、加入者側エッジL2SW20にRadiusクライアントを搭載し、アクセス網6に設置したProxy Radiusサーバ61で一旦認証情報を集約し、Proxy Radiusサーバ61から各プロバイダRadiusサーバ52に転送する方式をとれば、プロバイダエッジルータやプロバイダRadiusサーバの設定/データベース及び管理運用をほとんど変更なく使用できる。

【0070】また、アクセス網6のコアL2SW40は、タグを識別してフレームをMACブリッジング転送できればよく、IEEE802.1Q VLAN-Tagを用いるのであれば、市販で手に入るようなIEEE802.1Q対応のスイッチ装置を活用することができるので、容易にネットワークを構築することが可能である。

【0071】なお、本発明では、シグナリングのメカニズムとしてPPPoEを取り上げているが、必ずしもPPPoEに限定したものではなく、例えばIEEE802.1Xをポート単位の認証ではなく、ユーザ (MACアドレス) 単位の認証ととらえ、DHCP (Dynamic Host Configuration Protocol) サーバと密接に連携して、IPアドレスの割当及び解放動作を適切に行えば、PPPoEに代わるシグナリングメカニズムとして本発明において適用できる。

【0072】ここで、IEEE802.1X (Port Based Network Access Control) は、イーサネット上でポート単位のアクセスコントロールを行う方式であるが、ポート単位なので1ポートに複数端末が接続された環境では使用できない。ただし、ネゴシエーション中で送信元MACアドレスより相手装置を特定できるので、ポート単位ではなく、送信元MACアドレス単位でのアクセスコントロールととらえることにより複数端末にも対応可能である。

【0073】また、IEEE802.1Xは、IPアドレス割り当てのメカニズムを備えていない。一般には、DHCP (別プロトコル) によってIPアドレスが割り当てられ

る。したがって、本発明で適用する場合、ユーザがどのIPアドレスを使用しているか、またxSPを切り替える際などは、IPアドレス解放を適切に行うことが必要である(DHCPは一般にリースを受けたIPアドレスを継続使用しようとする)。

【0074】次に本発明の認証フェーズ時のシーケンスについて説明する。図6は認証フェーズ時のシーケンスを示す図である(なお、IP通信フェーズのシーケンスは図33、34に示す)。なお、Proxy Radiusサーバ61を用いて、認証に関する情報の中継制御を行った場合の動作シーケンスである(Proxy Radiusサーバ61の詳細は後述する)。

【0075】認証フェーズ時のPPPoEは大きく、PPPoE Discovery StageとPPP SessionStageに分かれる。また、ユーザ端末装置10のユーザ側セッション管理手段11と、加入者側エッジL2SW20の網側セッション管理手段21とで、認証フェーズの通信制御を行う。なお、以下は、PPPoEのシグナリングメカニズムを例としたシーケンスである。

【0076】〔S1〕ユーザ側セッション管理手段11と網側セッション管理手段21間でPADI(PPPoE Active Discovery Initiation)、PADO(PPPoE Active Discovery Offer)、PADR(PPPoE Active Discovery Request)を送受信する。そして、網側セッション管理手段21から送信されたPADS(PPPoE Active Discovery Session-confirmation)を、ユーザ側セッション管理手段11が受信することで、セッションIDが確立する。

【0077】〔S2〕LCPによりデータリンクが確立する。

〔S3〕網側セッション管理手段21からCHAP(Challenge Handshake Authentication Protocol) CHALLENGEが送信され、ユーザ側セッション管理手段11は、CHAP RESPONSEを返信する。CHAP RESPONSEには、ユーザ名@プロバイダ名、パスワードが含まれる。なお、CHAPとは、パスワードを暗号化してネットワークに送信する認証プロトコルのことである。

【0078】〔S4〕網側セッション管理手段21は、認証情報であるRadius Access-Request(ユーザ名@プロバイダ名、パスワード、CHAP CHALLENGE等を含む)をProxy Radiusサーバ61に送信し、Proxy Radiusサーバ61は、プロバイダRadiusサーバ52へRadius Access-Requestを中継する。

〔S5〕プロバイダRadiusサーバ52は、認証が成功すると(このように、実際の認証はプロバイダRadiusサーバ側で行われる)、Proxy Radiusサーバ61にRadius Access-Accept(ユーザ割当用のIPアドレス、対向(通信相手)のIPアドレス等を含む)を送信し、Proxy Radiusサーバ61は、網側セッション管理手段21へRadius Access-Acceptを中継する。

【0079】〔S6〕網側セッション管理手段21は、Radius Access-Acceptを受信するとCHAP SUCCESSをユーザ側セッション管理手段11へ送信する。

〔S7〕ユーザ側セッション管理手段11と網側セッション管理手段21は、IPCPにより、Radius Access-Acceptの受信値をもとに、IPアドレスネゴシエーションを行う。このIPCPの完了後にIP通信フェーズへ移行する。

【0080】次に加入者側エッジL2SW20について説明する。図7～図10は加入者側エッジL2SW20が有するテーブルを示す図である。図7のテーブルは、認証フェーズ時に参照する、ユーザの送信元MACアドレスとユーザのセッションIDの対応が示されるセッション管理テーブルT2aであり、図8のテーブルは、IP通信フェーズ時に参照する、ユーザのMACアドレスと接続先プロバイダ毎のタグとの対応が示されるVIDテーブルT2bである。

【0081】なお、本発明でいうところのVLAN-IDとは、仮想閉域網を一意に示すタグのことであり(VIDとも表記)、以降では、加入者側エッジL2SWが参照するVIDテーブルをMAC-VIDテーブル、プロバイダ側エッジL2SWが参照するVIDテーブルをポートVIDテーブルと呼ぶ。

【0082】また、図9のテーブルは、VLAN-ID毎に(プロバイダ毎に)独立したフォワーディング情報(転送情報)からなるフォワーディングテーブルT2cであり、図10のテーブルは、加入者側エッジL2SW20に設置されている各ポートの属性を示すポート属性テーブルT2dである。

【0083】セッション管理テーブルT2aは、(送信元)MACアドレス(ユーザ端末装置10のMACアドレス)、セッションID、状態及びユーザに割り当てるIPアドレス等のネゴシエーションパラメータの項目から構成され、認証フェーズの時に用いるテーブルである。

【0084】セッションIDは、図6で上述したPPPoE Discovery Stageにおいて確立するID(2バイト)を示し、状態は、認証フェーズか、またはIP通信フェーズであるかのいずれかの現在の通信状態を示す。また、ネゴシエーションパラメータは、エッジL2SWにユーザごとにあらかじめ登録しておくものではなく、例えば、ユーザに割り当てるIPアドレスなどは各xSPより指定され、仮想閉域網を一意に示すVIDは、VID情報を一元管理する通信管理サーバより指定される。

【0085】MAC-VIDテーブルT2bは、(送信元)MACアドレスとセッションID及びVLAN-IDの項目から構成され、IP通信フェーズの時に用いるテーブルである。なお、図では、セッション管理テーブルT2aとMAC-VIDテーブルT2bとを、別々のテーブルで構成しているが、1つのテーブルで構成して

もよい。

【0086】フォワーディングテーブルT2cは、(宛先)MACアドレスと、加入者側エッジL2SW20が持つ出力ポートの項目から構成され、アドレス学習及びエージングによりエントリ(テーブル内容)が追加・削除される。

【0087】また、フォワーディングテーブルT2cは、プロバイダ(VLAN-ID)毎に独立している。このため、1つの(宛先)MACアドレスから異なるプロバイダに出力することを防ぎ、不要なテーブル検索を抑制することが可能である。

【0088】ポート属性テーブルT2dは、ポート番号、受信フレーム、ブロードキャストフィルタリング及びタグ挿抜の項目から構成されて、ポート属性が示されるテーブルである。

【0089】加入者側エッジL2SW20へのポート入力時には、受信フレームの欄を見て、そのフレームを受け入れてよいか確認し、ポート出力時には、ブロードキャストフィルタリング及びタグ挿抜の欄を見て、どのような形式でフレームを出力するかを決定する。

【0090】ここで、図に示すポート属性テーブルT2dに対し、ポート番号1~4のポートがユーザ端末装置10側に接続するポートであり、ポート番号5~7のポートがアクセス網6側に接続するポートであるとする。この場合例えば、1番のポートでは、入力フレームがPPPoE、IP、ARP(Address Resolution Protocol)のいずれかのフレームであればそのフレームを取り込むことを表している(ARP処理については後述)。

【0091】また、5番のポートではIEEE802.1Q(すなわち、タグ付きフレーム)、GVRP、STPのいずれかのフレームであれば、そのフレームを取り込むことになる。

【0092】一方、ポート出力に対して、1番のポートからフレームを出力する場合には、ユーザ端末装置10側へフレーム出力することになるので、ブロードキャストフィルタリングをON(ブロードキャストしない)、タグはUntag(タグを外す)に設定し、また、5番のポートからフレームを出力する場合には、アクセス網6側へフレーム出力することになるので、ブロードキャストフィルタリングをOFF(ブロードキャストする)、タグはWithTag(タグの付加)に設定する。

【0093】ただし、プロバイダのポリシーによっては、ブロードキャストもユーザに届けたいという場合があり、ユーザ側ポートのブロードキャストフィルタリングをONにしてもよい。

【0094】ここで、ポート属性テーブルT2dの受信フレームの欄に、GVRP(GARP VLAN Registration Protocol)、STP(Spanning Tree Protocol)というプロトコル名があるが、GVRPはEthernetネットワーク

における、動的なVLAN構成情報を通知するプロトコルであり、STPはフレームのループを防ぐレイヤ2レベルで動作するEthernet制御プロトコルのことである。

【0095】このGVRPやSTPは、宛先MACアドレスとして特別なマルチキャストアドレス(GVRP:01-80-C2-00-00-21、STP:01-80-C2-00-00-00)を用いるので、アクセス網6内でGVRPやSTPを動作させるのであれば、図10のようにポート属性テーブルT2dの該当ポート欄に記入して、マルチキャストアドレスを受け入れ可能に設定しておけばよい。

【0096】図11は加入者側エッジL2SW20の動作概要を示す図である。加入者側エッジL2SW20は、ポート#1~#7を有し、ポート#1~#4がユーザ端末装置10-1~10-4にそれぞれ接続し、ポート#5~#7がアクセス網6側に接続する。また、ユーザ端末装置10-1~10-4のそれぞれのMACアドレスはA~Dとする。

【0097】ここで、ユーザ端末装置10-1は、MACアドレス=XのISPと接続中(IP通信フェーズ)である状態を示している。上述した各テーブルでこの状態を見ると、まず、MAC-VIDテーブルT2bより、(送信元)MACアドレス=Aならば、VLAN-ID=10であり、フォワーディングテーブルT2cにより、プロバイダ側への(宛先)MACアドレス=Xはポート#5から出力されることがわかる(タグ=10(VLAN-ID=10)が付加されてポート#5から出力される)。

【0098】ユーザ端末装置10-2は、MACアドレス=YのISPと接続中である状態を示している。上述した各テーブルでこの状態を見ると、フォワーディングテーブルT2cにより、ユーザ側への(宛先)MACアドレス=Bはポート#2から出力されることがわかる(タグ=11(VLAN-ID=11)が外されてポート#2から出力される)。

【0099】ユーザ端末装置10-3は、MACアドレス=ZのISPと接続トライアル中(認証フェーズ)である状態を示している。この段階では、セッション管理テーブルT2aを用いて、PPPoEの接続制御が行われる。

【0100】また、ユーザ端末装置10-4は、MACアドレス=YのISPとの接続中にIPX(Internet Packet Exchange)フレームを送信しようとしている状態を示している。この場合、ポート属性テーブルT2dでは、ポート#4の受信フレームの欄にIPXは設定されていないので、IPXフレームは、加入者側エッジL2SW20で受け入れられないことになる。

【0101】次に加入者側エッジL2SW20のブロック構成及び動作フローについて説明する。図12は加入者側エッジL2SW20のブロック構成を示す図であ

る。加入者側エッジL2SW20の処理は、フレーム入力処理、フォワーディング処理、フレーム出力処理に大きく分かれる。

【0102】フレーム入力処理では、フレーム入力時、まずETHER-TYPE抽出手段201はフレームタイプを識別し(また、TPIDからタグ付きか否かも識別する)、ポート属性テーブルT2dをチェックする。このとき、入力を認めないフレーム(例えば、IPXフレームなど)であれば廃棄する。

【0103】そして、PPPoEのフレームであれば、CPU202に渡して、セッション管理テーブルT2aをもとにPPPネゴシエーションを行う(RFC1661で規定された状態遷移図にしたがったネゴシエーションを行う。この状態遷移に関する内容は省略する)。

【0104】また、認証フェーズ完了後のIP通信フェーズ接続開始の状態であれば、CPU202は、ユーザのMACアドレスを該当プロバイダのMAC-VIDテーブルT2bに登録し、接続終了であれば、MAC-VIDテーブルT2bより削除する。

【0105】そして、入力フレームが、IEEE802.1Qのタグが付加されていないフレームであれば、VLAN-IDチェック手段204は、MAC-VIDテーブルT2bからユーザの接続先プロバイダに対応したVLAN-IDを抽出する。もし、MAC-VIDテーブルT2bにエントリがなければ、そのユーザは未認証等でIP通信フェーズではないとみなしフレームを廃棄する。

【0106】一方、IEEE802.1Qフレーム(タグ付きフレーム)の場合は、ETHER-TYPE抽出手段201は、VIDフィールドからVLAN-IDを認識し、ペイロード抽出手段203は、IEEE802.1Qタグフレームを受信した場合、ETHER-TYPEを抽出し、0x0800や0x86DDであれば主信号フレームなのでそのままフォワーディング処理へ、0x0806のARPなどの場合は、CPU202へ回す。

【0107】フォワーディング処理の出力ポート決定手段205では、宛先MACアドレスにしたがって、VLAN-ID毎に独立したフォワーディングテーブルT2cから出力ポートを決定する。この際、送信元MACアドレス及び入力ポートからアドレス学習及び一定時間後にエージングを行う。

【0108】もし、宛先MACアドレスが自分宛て(例えばProxy Radiusサーバ61からのRadius Access-Acceptなどが該当)であれば、CPU202に回して処理を行う。フレーム出力処理の出力処理手段206では、再度、ポート属性テーブルT2dにしたがって、タグの挿抜及びブロードキャストフレーム出力の可/不可を決定してフレームを出力あるいは廃棄したり、ユニキャストのフラッディングのフィルタリングを行う。

【0109】このように、加入者側エッジL2SW20では、受信フレームに対し、ETHER-TYPEを見て、制御

フレームであるか主信号フレームであるかを判断し、制御フレームならばCPU202に回して処理し、主信号フレームならば、ハードウェアで処理することにより、高速なIPデータ通信が可能である。

【0110】図13は加入者側エッジL2SW20の全体動作を示すフローチャートである。なお、ステップS12はソフトウェア処理、ステップS11とステップS13～ステップS18はハードウェア処理である。

〔S11〕ETHER-TYPEを抽出し、抽出した値にもとづき、ステップS12～ステップS15のいずれかへ行く。

【0111】〔S12〕PPPoEならばPPPoEネゴシエーションを行う。

〔S13〕ポート属性にない場合は廃棄する。

〔S14〕IPoEならば送信元MACアドレスよりMAC-VIDテーブルT2bを引く。エントリにあればステップS18へ、なければステップS16へ行く。

【0112】〔S15〕タグ付きフレームならば、VIDフィールドより、VLAN-IDを認識する。

〔S16〕エントリにないので廃棄する。

〔S17〕ペイロードを抽出する。

〔S18〕フォワーディング処理/出力処理を行う。

【0113】図14は加入者側エッジL2SW20のPPPoEネゴシエーションの動作を示すフローチャートである。

〔S21〕PPPoEのフレームを受信すると、送信元MACアドレスより、セッション管理テーブルT2aを引く。

〔S22〕RFC1661で規定された状態遷移にしたがって、ユーザに返信またはProxy Radiusサーバ61へRadius Access-Requestを送信する。

【0114】〔S23〕新しい状態(State)をチェックする。接続終了ならばステップS24へ、IP通信フェーズならばステップS25へ、その他ならば終了する。

〔S24〕MAC-VIDテーブルT2bから該当エントリを削除する。

〔S25〕MAC-VIDテーブルT2bへ該当エントリを登録する。

【0115】図15は加入者側エッジL2SW20のフォワーディング処理/出力処理の動作を示すフローチャートである。

〔S31〕フォワーディング処理時、該当のVLAN-IDのフォワーディングテーブルT2cを検索する。

〔S32〕エントリが存在するか否かを判断する。あればステップS33へ、なければステップS34へ行く。

【0116】〔S33〕ポート属性テーブルT2dにもとづいてタグ挿抜を行う。そして、フレームを出力する。

〔S34〕入力ポート以外の各ポートでポート属性テー

ブルT2dより、ブロードキャストフィルタリング処理を行う。

【S35】フィルタリングがONならば廃棄する。

【0117】次にユーザ端末装置10について説明する。図16はユーザ端末装置10の構成を示す図である。なお、図におけるIP層及びその上位層、またMAC層に関しては、既存のプロトコルスタックをそのまま使用可能である（本発明の主信号送受信手段12は、TCP層、IP層、MAC層を通じての処理である）。また、図17には従来のユーザ端末におけるプロトコルスタックを示す。

【0118】プロバイダへの接続開始時、まず、ユーザ側セッション管理手段11より、図6で上述したPADIパケット（PPPoE Active Discovery Initiationにおいて、接続開始時に使用）を送出する（認証フェーズ完了までは、通常のPPPoE動作と同じ）。以降、ユーザ側セッション管理手段11が持つユーザ側セッション管理テーブル（図18に例を示す）を参照して、ネゴシエーションを行い、ユーザ認証では、ユーザが接続するプロバイダをユーザIDが「ユーザ名@プロバイダ名」の形式で指定して認証フレームを送出する。

【0119】そして、認証成功後、IPCPネゴシエーションを経て、認証フェーズを完了し、IP通信フェーズでは、割当を受けたIPアドレスをEthernetインタフェースに設定し、また対向アドレス（プロバイダエッジルータのIPアドレス）をデフォルトルートとしてルーティングテーブル（図19にルーティングテーブルの例を示す）に設定してIPデータ通信をIPoE形式で行う。

【0120】ただし、ネットマスクに関しては、接続したプロバイダサブネットのサブネットマスク値に従う。すなわち同一サブネットの場合は、プロバイダエッジルータを経由せずに、直接IPoEフレームを送信する。

【0121】また、IP通信フェーズでは、接続性確認のフレームを定期的に送出する。認証フェーズで、PPPoEのネゴシエーションを行った加入者側エッジL2SW20に対しては、接続セッションの維持のため、図20に示すような接続性確認フレーム（LCP Echo-Request）を送信する。

【0122】そして、加入者側エッジL2SW20は、LCP Echo-Requestに対して、LCP Echo-Replyを返し、ユーザが接続継続中であることを確認する。これにより、加入者側エッジL2SW20が一定期間LCP Echo-Requestが受信できない場合、あるいは反対にユーザ端末装置10がLCP Echo-Replyを一定期間受信できない場合にセッションが終了したとみなすことにより、回線断などの不慮の事態にも異常をきたすことなくセッションを終了させることができる。

【0123】また、接続性確認を行う場合、ユーザ端末装置10は、プロバイダエッジルータ（IPCPで指定

を受けた対向アドレス）に対しては、Ping(ICMP Echo-Request)を送信する。これはコアL2SW、加入者側エッジL2SW20、プロバイダ側エッジL2SW内の、フォーワーディングテーブルのエントリにおけるエージングを回避するためである。

【0124】そして、ユーザ端末装置10は、接続終了時には、接続終了を示す制御フレームを送信する。PPPoEであれば、図21のような接続終了フレーム（LCP Terminate-Request）を送信する。

【0125】そして、加入者側エッジL2SW20は、これを受けて、ユーザのMACアドレスに関するエントリをセッション管理テーブル及びMAC-VIDテーブルより削除し、LCP Terminate-Ackを返す。その後、ユーザ端末装置10は、切断フレームであるPADTパケット（PPPoE Active Discovery Terminate、PPPoE接続の終了を通知する際に使用）を送信して接続が終了する。また、このとき、ユーザ端末装置10では、Ethernetインタフェースに設定したIPアドレスを削除し、ルーティングテーブルも削除する。

【0126】また、ユーザ端末装置10内のユーザ側セッション管理手段11は、一定時間IPデータ通信が行われない場合に、自動的に接続を終了させることが可能な通信監視機能を持つ。ただし、実際に接続を終了するのは、ユーザが任意に設定可能とする。

【0127】なお、ユーザの接続先プロバイダが固定の場合などには、あらかじめユーザID（ユーザ名@プロバイダ名）及びパスワードを記憶させておき、ユーザ端末装置10の起動時には、自動的にユーザ側セッション管理手段11より、セッション制御を開始することにより、常時接続的な通信を行うことも可能である。

【0128】また、ユーザ側セッション管理手段11は、グローバルユニークなMACアドレスが設定されたEthernetインタフェースを持つものであれば、例えば、家庭内LANを構成している場合には、ゲートウェイルータ等に搭載されてもよい（図22）。この場合は、上記のようにあらかじめユーザIDとパスワードをゲートウェイに設定しておき、家庭内LAN側からのインターネット向けのIPパケットを受信したときに、ゲートウェイから自動的に発呼を行うことが可能である。

【0129】図23はユーザ端末装置10の動作を示すフローチャートである。ユーザ側セッション管理手段11による全体動作を示している。

【S41】制御フレームによるネゴシエーションを行う（認証、IPアドレス割当等）。

【0130】【S42】認証フェーズ完了か否かを判断する。完了ならばステップS43へ、完了でなければステップS41へ戻る。

【S43】IPoEで主信号フレームを送受信すべく、IPアドレス、ルーティングテーブル等の設定を行う。

〔S44〕IP通信の通信監視制御を行う。

【0131】〔S45〕接続完了か否かを判断する。完了ならばステップS47、完了でなければステップS46へ行く。ここで、接続完了は、通常はユーザが明示的に行う。ただし、接続性確認フレームに対する返信が得られない場合、あるいは通信監視制御によるIPデータ通信の無通信検出により、接続完了処理を行うことも可能である。また、ユーザのパスワードミスなどにより、加入者側エッジL2SW側から接続完了処理が行われる場合もある。

【0132】〔S46〕接続性確認のため、一定時間ごとに、加入者側エッジL2SWに制御フレーム(LCP Echo Request)を、プロバイダ側エッジL2SWにPing(ICMPEcho Request)を送信する。

〔S47〕設定した、IPアドレス及びルーティングテーブル等を削除する。

〔S48〕接続完了を示す制御フレーム(LCP Terminate Request)を送信する。

〔S49〕加入者側エッジL2SWより、LCP Terminate ACKの受信後、PADTを送信する。PADTを送信して切断となる。

【0133】次にARPの制御に関し、最初に一般のARP動作について説明する。IPoEでフレームを送信する際には、通信を行う相手のMACアドレスを知る必要がある。その際には、まずARP Requestを送信し、通信相手の方は、自らのMACアドレスを返信メッセージに格納して、ARP Reply(ユニキャスト)として返信する。

【0134】これでIPアドレスとMACアドレスの対応を表すARP Tableにエントリを持つ(ARPキャッシュと呼ばれ、一定期間保持される)ことになるので、IPoEでフレームを送受信することが可能となる。

【0135】図24はARP Request及びReplyのフォーマットを示す図である。ARP Request送信端末は、送信元MACアドレスを自らのMACアドレスとし、Src Hw Addr及びSrc Prot Addrフィールドにも自らのMACアドレスとIPアドレスを格納して送信する。そして、知りたいのは、Tgt Prot Addrに対応するIPアドレスを持っている端末のTgt Hw Addr(MACアドレス)である。

【0136】ARP Reply送信端末は、宛先MACアドレスを上記のARP Request送信端末、送信元MACアドレスを自らのMACアドレスとし、Src Hw Addr及びSrc Prot Addrに自らのMACアドレスとIPアドレスを格納して送信する。

【0137】図25は一般のARPの動作を示す図である。ARP Requestを受信する端末、ARP Replyを受信する端末はともに、Src Hw Addr及びSrc Prot AddrフィールドからARPエントリをキャッシュする。すなわち、ARP Requestを受信した場合もARPエントリがキャッシュされ

ることになる。

【0138】したがって、ARP Requestはブロードキャストフレームであるため、ブロードキャストドメイン内の全端末すなわち、アクセス網6経由で同一プロバイダに接続している(同一サブネットの)全ユーザに送信され、受信した端末は送信元端末のARPエントリをTableにキャッシュしてしまう。

【0139】この動作は企業ネットワーク等のLANセグメントでは問題ないが、プロバイダ接続ユーザは、インターネットやコンテンツなどのサービスを目的としているのであるため、プロバイダ接続ユーザ間での通信は本来の目的ではなく、ブロードキャストドメイン内の全端末にARP Requestが送信されるのは、セキュリティ的にも問題がある。

【0140】また、ARPをフィルタリングすると、仮にブロードキャストドメイン内のユーザ間でチャット等のP-to-P接続を行いたい、というニーズがあった場合にMACアドレスを知ることができなければ通信を行うことは不可能である。

【0141】また、一旦、プロバイダエッジルータに転送して、プロバイダエッジルータがあらためて相手ユーザに転送する方法も技術的には可能であるが、この場合、プロバイダエッジルータの入出力ポートが同じであり、その都度ICMPエラーパケット(ICMP Redirect)が送出され、プロバイダエッジルータに負担がかかってしまう。すなわち、ARP Request等のブロードキャストフレームは、ブロードキャストドメイン内の全端末に送信するのではなく、本来送るべき相手にのみ送信するといった制御が必要となる。

【0142】次に本発明のアドレス解決手段によるARP制御について説明する。本発明では、各加入者側エッジL2SWは、送信元MACアドレスでセッションを管理し、認証フェーズでユーザ端末装置10にIPアドレスを割り当てるので、どのMACアドレスの端末がどのIPアドレスを保持しているかを表すARPエントリに相当するテーブル(図26:以降、ARPリレーテーブルと呼ぶ)を作成することが可能である。

【0143】そこで本発明では、ユーザから送信されたARPフレーム(ETHER-TYPE 0x0806)について、加入者側エッジL2SWがMAC-VIDテーブルにて認証の確認及びVLAN-ID抽出後、ARPリレーテーブル(VLAN-ID毎に持つ)を参照して、Tgt Prot Addr(IPアドレス)で検索し、エントリがあれば本来のホストに代わってARP Replyを返信することの特徴とする。

【0144】このとき、送信元MACアドレスは加入者側エッジL2SW20のMACアドレス、Src Hw AddrとSrc Prot AddrはARPリレーテーブルでヒットしたARPエントリである。

【0145】もし、エントリになかった場合には、アクセス網6側に対してはタグを付加してブロードキャスト

のまま送信し、ユーザ側には送信しない(本発明の動作は、加入者側エッジL2SW20のポート属性テーブルの設定で、ユーザ側ポートのブロードキャストフィルタリングを「ON」、アクセス網6側のポートを「OFF」とすることにより可能である)。

【0146】アクセス網6内の各エッジL2SW(加入者側及びxSP側)は、このタグ付きARP Request をアクセス網6側から受信し、同様に対応するVLAN-IDのARPリレーテーブルを引き、エントリを持つ加入者側エッジL2SWがARP Replyを返す。

【0147】なお、本発明の動作はいわゆるProxy ARPとは異なる。Proxy ARPはルータが行う動作で、ユーザからのARP Requestに対して自身(ルータ)のMACアドレスを返し、IPフレームは実際にはL3ルーティングにより転送する(図27)。

【0148】一方、本発明の動作は、ARP Replyは本来のホストがもつエントリである。したがってIPフレームはレイヤ2(MACブリッジング)で転送する。このARPリレーテーブルは、ユーザが異なるプロバイダに接続するたびに、IPアドレスが変わるため、エントリも変化する。

【0149】したがって、このテーブルはユーザの認証フェーズ完了時に登録され、接続終了時には削除する。ただし、プロバイダエッジルータのIPアドレス及びMACアドレスは機器を変更したりしないかぎりには同一であるため、プロバイダエッジルータのエントリは、プロバイダ側エッジL2SWが固定的に保持するものとする。

【0150】図28は本発明のARPの制御を示す図である。ARPリレーテーブルは、通常のARP動作(ARP Request/Reply受信)でキャッシュすることはしない。したがって、あるユーザ(Pとする)がISP-YエッジルータのARPエントリを知ろうとした場合には、ISP-Yエッジルータが接続されたプロバイダ側エッジL2SWがARP Reply を返し、同一プロバイダ 接続ユーザ(Qとする)のARPエントリを知ろうとした場合には、ユーザQが接続された加入者側エッジL2SW20がARP Replyを返すことになる。

【0151】存在しないエントリに対するARP Requestに対しては、どの加入者側エッジL2SW20もARP Replyを返さず、アクセス網6から外に出ることなく廃棄されるので、ARP Request送信元端末のARPエントリが同一プロバイダ接続ユーザにブロードキャストされてしまうことはない。

【0152】また、アクセス網6内は(VLAN内にかぎり)ブロードキャストのまま送出するわけであるが、GVRPやSTPとの併用により、不要なポートへの送出やフレームのループ等は発生しない。

【0153】また本発明の動作は、プロバイダのポリシーにより、例えばプロバイダエッジルータのARPエントリ

リ以外は返答しない(すなわちプロバイダ側エッジL2SW30以外は代理でARP Replyを返さない)よう設定すれば、同一プロバイダ接続ユーザ間の通信を禁止することができ(すなわち、プロバイダ接続のみ可)、あるいはARPリレー機能をそのものをOFFにして全ユーザにARP Requestを透過させて普通のLANセグメント同様のネットワークを構成することも可能である。

【0154】また、ARPフレームも認証状態を確認して、VLAN-IDの識別を行うため、各プロバイダのポリシーに応じてARPリレー機能をON/OFFしても、プロバイダ毎の仮想閉域網に閉じた接続は保持される。

【0155】なお、IPv6では、ARP相当の動作は、ICMPv6で動作するNeighbor Discovery に統合された。したがってIPv6に移行した場合は、加入者側エッジL2SW20内部の各ブロックでは、IPv6フレーム(図29)におけるNext Headerフィールドを抽出して、ICMPv6(=58)の場合にCPUに回して処理を行うことになる。それ以外の場合(TCP=6、UDP=17 など)にはそのままハードウェア処理を行う。

【0156】次に本発明のARP制御に対するさらなる付加処理について説明する。上記では、加入者側エッジL2SW20でARPリレーテーブルにヒットした場合、本来のユーザに代わってARP Replyを返すことを特徴とした。しかし、図28のように端末Pとプロバイダエッジルータ(ISP-Yエッジルータ)が通信を行う場合、端末PがARP Replyを受けてエントリをキャッシュし、ISP-Yに対してIPOEで送信し、ISP-Yエッジルータが端末Pに返信しようとした場合、ISP-Yエッジルータには端末Pのエントリがキャッシュされていないため、ISP-Yエッジルータも端末PのMACアドレスを知るためのARP Requestを送出する必要がある(IPデータフレームの送受信ではARPキャッシュされない)。

【0157】代理応答しない本来のARPの動作であれば、ARP Requestを受信した端末は、Src Hw Addr及びSrc Prot Addrからエントリをキャッシュするため、1回のARP Request/Reply のやりとりで済む(図30)。

【0158】そこで、加入者側エッジL2SW20でARPリレーエントリにヒットした場合、ARP Request の送信元MACアドレス(ブロードキャスト)を該当端末のMACアドレス(ユニキャストアドレス)に変換して該当端末にのみ転送する。

【0159】そのARP Requestを受け取った端末は、送信元端末に対してARP Replyを返す。このようにすれば、1回のARP Request/Replyのやりとりでお互いにARP エントリをキャッシュすることが可能となる。ここで、図31、32は本発明のARP制御に関する動作シーケンスを示す図である。また、図33、34にIP通信フェーズ及び接続性確認処理を行うシーケンス図である。

【0160】次に本発明のプロバイダ側エッジL2SW30について説明する。プロバイダエッジルータが接続されたプロバイダ側エッジL2SW30のポートは、一般にプロバイダ毎に固定である。

【0161】また、プロバイダエッジルータの二重化対応などで障害時にはバックアップルータに切り替わる場合なども考えられるため、プロバイダからのフレームを識別するのは、加入者側のようにMACアドレスベースではなく、ポートベースで行うことが望ましい。

【0162】したがって、プロバイダ側エッジL2SW30では、ポートとVLAN-IDとの対応を示すポートVIDテーブル(図35)を固定的に持ち、プロバイダからのフレームは入力ポートよりプロバイダを識別し、プロバイダ毎のフォワーディングテーブル(形式は加入者側エッジL2SWと同じ)及びポート属性テーブル(形式は加入者側エッジL2SWと同じ)から対応するタグを付加してアクセス網6に転送し、アクセス網6側からはタグを外してプロバイダに転送する(プロバイダ側エッジL2SW30に対して、ユーザ→プロバイダの制御は出力処理手段31、プロバイダ→ユーザの制御は、送信処理手段32で行う)。

【0163】なお、プロバイダ側エッジL2SW30は、加入者側エッジL2SW20と違い、制御フレームをハンドリングしない。なぜなら、ユーザのセッション管理は、加入者側エッジL2SW20で行っており、未認証ユーザ等のアクセスも遮断しているためである。このため、不正アクセスがプロバイダに対して行われることはない。

【0164】また、プロバイダエッジルータ51のARPエントリは障害等で機器そのものを交換しないかぎり、常に一定(プロバイダエッジルータ51のIPアドレスは固定でMACアドレスもEthernetインタフェースを交換しないかぎり固定)であるため、プロバイダ側エッジL2SW30は、プロバイダエッジルータ51のARPリレーエントリを静的に持つものとする(図35にARPリレーテーブル、その他のテーブル構成を示す)。

【0165】本発明のARPリレー処理では、プロバイダエッジルータ51に対するARP Requestは、プロバイダが接続されたプロバイダ側エッジL2SW30が代理でARP Replyを返す。または、プロバイダが接続されたプロバイダ側エッジL2SW30がユニキャスト変換してプロバイダエッジルータ51に転送する。

【0166】図36にプロバイダ側エッジL2SW30のモデル図を示す。なお、図のとおり1台のプロバイダ側エッジL2SW30ですべてのプロバイダと集中接続しなければいけないというわけではない。また、図37にプロバイダ側エッジL2SW30の機能ブロック、図38にプロバイダ側エッジL2SW30の動作を示すフローチャートを示す。

【0167】次に本発明の通信管理サーバ61の認証制

御手段について説明する(すなわち、Proxy Radiusサーバ61について説明する)。本発明に関わる通信システムでは、アクセス許可(ユーザの主信号フレームを通すか通さないかの判断)、接続先プロバイダの振分け(タグを付加してアクセス網6に転送)及びシグナリング処理(PPPoEハンドリング)はユーザ端末装置10が接続された加入者側エッジL2SW20で行うが、ユーザの実認証はプロバイダが持っているデータベースで照合することになる。

【0168】このような認証に用いられるプロトコルとしてはRadius(RFC2865 ~2869)が挙げられる。RadiusはUDP (User Datagram Protocol) で動作し、ユーザIDやパスワードをAttribute(属性値)として扱い、Radius Access-RequestとしてRadiusクライアント(この場合、加入者側エッジL2SW20側に設置)がプロバイダRadiusサーバ52に送信して、プロバイダのデータベースで認証し、認証が成功した場合はRadius Access-Accept、失敗した場合にはRadius Access-Rejectが返される。なお、Radius Access-AcceptにはAttributeとしてユーザに割り当てるIPアドレス等が含まれる。

【0169】またRadius Accounting-Requestによってユーザの接続時間、通信データ量などをプロバイダRadiusサーバ52に送信することによりプロバイダ側で接続に関する統計情報等を管理することができる。

【0170】Radiusは、ADSL接続等で広く用いられており、本発明でも認証プロトコルとして用いた例を上述したが、その他の認証プロトコルとしてTACACS(RFC1492)やLDAP(RFC2251)あるいはRadiusの次世代プロトコルとして標準化が進められているDiameterなど同様の機能を実現するプロトコルを利用してもよい。なお、上記の説明では、実認証をCHAPとしたが、本発明はCHAPに限るものではない(ワンタイムパスワードや指紋認証等)。

【0171】次にアクセス網6内に設置したProxy Radiusサーバ61による認証フレーム転送制御方式について説明する。各加入者側エッジL2SW20は、ユーザから受信したユーザID(ユーザ名@プロバイダ名)及びパスワードをRadius Access-Requestとして、認証情報を表すタグ(認証タグ)を付加してEthernetフレームでProxy Radiusサーバ61に対して送信する。

【0172】一方、アクセス網6内では、認証タグを付加したフレームを認証VLANと識別し、GVRP等公知のプロトコルを用いて、Proxy Radiusサーバ61に正しく転送されるよう設定しておく。これによりアクセス網6内のコアL2SW40では、タグにもとづいて、認証情報を運ぶフレームであることを識別するので、認証情報が第三者に漏れることなくProxy Radiusサーバ61に転送されることになる。

【0173】そして、Proxy Radiusサーバ61は、プロバイダ名とVLAN-ID及び各プロバイダRadiusサーバ52のIPアドレス等の対応を示すプロバイダ管理テ

ープルを持ち、「ユーザ名@プロバイダ名」からプロバイダを識別して、各プロバイダRadiusサーバ2に、上記Radius Access-Request を、対応するプロバイダのタグを付加したEthernetフレームとして送信する(プロバイダ側エッジL2SW30ではタグを外して転送する)。

【0174】プロバイダRadiusサーバ2からはProxy Radiusサーバ61に対してRadius Access-Accept(あるいはRejectの場合もある)が送られてくる。Proxy Radiusサーバ61は、このRadius Access-AcceptにプロバイダのVLAN-IDを示すAttributeを追加して、加入者側エッジL2SW20に転送する。加入者側エッジL2SW20は認証フェーズ完了時に、Attributeで受信したVLAN-ID値を用いてMAC-VIDテーブルに登録する。

【0175】したがって、加入者側エッジL2SW20は、単一のProxy Radiusサーバ61とのみ通信すればよく、また主信号フレームに付加するプロバイダのVLAN-IDもRadius Access-Acceptで示されるため、加入者側エッジL2SW20でプロバイダの追加/削除に伴う登録作業を行う必要がなく(Proxy Radiusサーバ61で一元管理すればよい)、管理工数や加入者側エッジL2SW20に搭載するメモリ量が削減できる。また、プロバイダRadiusサーバ2は、単一のRadiusクライアントとのみ通信すればよいので、プロバイダの設定に大きな変更が加わることはない(従来方式では、B-RASが単一のRadiusクライアントとして、各プロバイダRadiusサーバと通信していた)。

【0176】また、加入者側エッジL2SW20とProxy Radiusサーバ61間の通信では認証タグを付加し、Proxy Radiusサーバ61とプロバイダRadiusサーバ2間の通信では、対応するプロバイダのタグを付加して転送するので、セキュリティも確保される。

【0177】図39にProxy Radiusサーバ61の動作を示し、Proxy Radiusサーバ61で管理するテーブルを図40に示す。また、図41はユーザからの認証要求から認証成功までの動作シーケンスを示す図である。

【0178】次に複数接続先への接続制御について説明する。従来、PPPoEでは、PPPoE Discovery Stageでセッション毎にユニークなID(Session-ID)が確立される。そして、PPP Session Stageでは、確立したSession-IDを設定してネゴシエーション及びIPパケットのカプセル化転送を行う。したがって、PPPoEでは送信元MACアドレスとSession-IDからセッションを識別することにより、複数プロバイダに同時接続を行うことが可能である。

【0179】一方、本発明では、認証フェーズにおけるシグナリング処理には、PPPoEのメカニズムを用いるため同様に複数セッションを管理することは可能であり(図42)、ユーザ端末装置10に搭載したセッション

管理機能においても、複数セッションを管理し、複数プロバイダに対して主信号フレームを送信することが可能である(図43)。

【0180】ただし、加入者側エッジL2SW20において、主信号フレームはIPoEで受信するため、Session-IDフィールドが無く、送信元MACアドレスでMAC-VIDテーブルを引くと、複数のVLAN-IDにマッチしてしまい、該当の接続先プロバイダを一意に識別することが出来ない(図44)。

【0181】そこで本発明では、加入者側エッジL2SW20において、送信元MACアドレスだけでなく、複数VLAN-IDにマッチした場合には、宛先MACアドレスで接続先プロバイダを一意に絞るようにする。

【0182】宛先MACアドレスからVLAN-IDを識別するためのテーブル(宛先MACアドレステーブルと呼ぶ)の作成は、上述したARPリレー処理を応用する。また、上述のとおりIPoEでフレームを送信するために、相手のMACアドレスを知るため、先立ってARP Requestを送信する(ARPが解決できなければ通信できない)。

【0183】そして、例えば、ARPリレーテーブルにヒットしたエッジL2SWが代理でARP Replyを返す。このARP Replyはユニキャストなので、受信したエッジL2SWはARP ReplyのSrc Hw Addr 値とタグ(アクセス網6側からは該当プロバイダのタグを付加されて送られてくる)をもとに宛先MACアドレステーブルに登録する。

【0184】このような動作により、複数同時接続時にもあらかじめARP Replyにより宛先MACアドレステーブルに登録されているため、該当接続先を一意に識別することが可能となる。ただし、宛先MACアドレステーブルの検索は、あくまで複数同時接続時(送信元MACアドレスでVIDテーブルを引いて複数マッチした場合)に限る。これは単一プロバイダ接続時には、送信元MACアドレスだけで一意に識別可能であり、不要な検索を防ぐためである。また、アクセス網6側からの下りに関しては、タグより一意に識別可能であり、複数同時接続時でも動作に変更はない。

【0185】なお、ユーザの接続終了時は、PPPoEフレーム(LCP Terminate-Request、図19)で行うため、MAC-VIDテーブルの削除は、送信元MACアドレスとSession-IDより該当のエントリのみを削除する。本発明の動作を加えた、加入者側エッジL2SW20の動作を示すフローチャート(メイン、ARPリレー処理)をそれぞれ図45、図46に示す。

【0186】次に複数接続先への同時接続時に、ユーザ端末装置10のレイヤ2アドレスに加えて、レイヤ3アドレス(IPサブネット)より、ユーザの主信号フレームの接続先を一意に識別する場合について説明する。

【0187】IPアドレスは、IPv4もIPv6もネットワーク部(IPサブネット)とホスト部により構成さ

れ、プロバイダに接続した際、アドレスプールから割り当てられるIPアドレスは、IPサブネットに関してはプロバイダ毎に一意であり、複数プロバイダ同時接続時、IPサブネットを見ればどのプロバイダ宛てのフレームかを判断することが可能である。

【0188】したがって、本発明では、加入者側エッジL2SW20がIPサブネットとVLAN-IDの対応を示すIPサブネットテーブルを持ち、送信元MACアドレスでVLAN-IDを引いて複数マッチした場合、IPサブネットにより該当の接続先を一意に識別することを特徴とする。

【0189】なお、IPサブネットは、プロバイダ毎に一意で、かつ固定であるため、各エッジL2SWはIPサブネットテーブルを固定的に持つものとする(図47)。ただし、プロバイダの追加時にはProxy Radiusサーバ61よりSNMPなどの管理プロトコルにより各エッジL2SWに設定することも可能である。

【0190】なお、本発明の場合も接続先プロバイダの識別は、あくまで送信元MACアドレスによるVIDテーブルの検索が基本である(テーブルにエントリがない場合は未認証とみなして廃棄する)。

【0191】そして、複数マッチした場合に限り、IPサブネットテーブルよりプロバイダを一意に絞る。本発明の動作を加えた、加入者側エッジL2SW20の動作を示すフローチャート(メイン)を図48に示す。

【0192】次に複数同時接続に対し、認証フェーズにおいて、IPアドレスの割当を行うとともにアクセス網6内でプロバイダを一意に識別するタグをユーザ端末装置10に配布して、ユーザ端末装置10からタグを付加したかたち(IEEE802.1Qフレーム)で主信号フレームを送信する場合について説明する。

【0193】このような制御を行うことで、加入者側エッジL2SW20では、送信元MACアドレスによるMAC-VIDテーブルの検索で複数マッチした場合(エントリがない場合は廃棄)に、タグを見て一意に絞ることが可能となる。

【0194】なお、タグを見ただけで接続先を一意に判別することは可能であるが、正しく認証されているかは判断できない(不正にタグを付加して送信してきたのかもしれない)ので、送信元MACアドレスでMAC-VIDテーブルのチェックは必須である。あるいは、タグから接続先プロバイダを一意に識別後、MAC-VIDテーブルに該当のエントリがあるかチェックする方法でも構わない。

【0195】この場合、加入者側エッジL2SW20のポート属性テーブル(図10)の設定としては、ユーザ側ポートでもIEEE802.1Qフレームを受信可能にし、タグ挿抜を「With Tag」に設定することで対応することができる。

【0196】なお、プロバイダ側エッジL2SW30で

は、これまでと同様にタグを外してプロバイダエッジL2SW31に転送する。そしてプロバイダ側からのフレームは入力ポートから対応するタグを識別/付加してアクセス網6を転送する(図50)。これらの動作を加えた加入者側エッジL2SW20の動作を示すフローチャート(メイン)を図49に示す。

【0197】なお、PPPoEでカプセル化する場合と異なり、IEEE802.3ac-1998準拠のEthernetインタフェースカードであれば、ユーザ端末装置10でIEEE802.1Q VLAN-Tagを付加した場合でもMTUが1500バイトのIPパケットの送受信が可能である。

【0198】次に本発明の通信管理サーバのセッション管理手段について説明する(以降の説明ではセッション管理サーバと呼ぶ)。加入者側エッジL2SW20では、ETHER-TYPEでフレームを判別し、主信号フレームはアクセス許可(ユーザの主信号フレームを通すか通さないかの判断)及び接続先プロバイダの振分け(タグを付加してアクセス網6に転送)をハードウェア処理、制御フレームによるシグナリング処理(PPPoEハンドリング)をソフトウェア処理で行うことを特徴としたが、ここでは、シグナリング処理に関しては、アクセス網6内に設置したセッション管理サーバで集中的に行い、主信号フレーム処理と制御フレーム処理を装置的に分離処理する場合について説明する。

【0199】上述したように、PPPにおける制御情報のネゴシエーションは、ユーザ毎に条件も異なるため処理負荷が大きい。本発明ではユーザ端末装置10が接続された加入者側エッジL2SW20にて分散処理しているため、B-RASに比べると負荷は小さいものの、加入者側エッジL2SW20の負荷は小さいほうが望ましい。

【0200】そこで、加入者側エッジL2SW20にて制御フレームをハンドリングするのではなく、主信号フレーム同様にハードウェア処理でアクセス網6内に設置したセッション管理サーバに転送する。

【0201】セッション管理サーバは上述の図7で示したセッション管理テーブルを持ち、ユーザとネゴシエーションを行う。ただし、アクセス許可及び主信号フレームの接続先プロバイダへの振分けは、加入者側エッジL2SW20で行うため、認証フェーズ完了後、セッション管理サーバからユーザが接続された加入者側エッジL2SW20を設定(MAC-VIDテーブルの遠隔設定)する必要がある。

【0202】設定自体はSNMPなど既存の管理プロトコルで可能であるが、加入者側エッジL2SW20を経由して転送されてきたユーザの制御フレームには、加入者側エッジL2SW20を識別する情報が含まれていないため、どのエッジL2SW配下にユーザが接続されているか判断できない。

【0203】そこで、制御フレームに関しては、加入者

側エッジL2SW20を識別するタグを付加してセッション管理サーバに転送する。すなわち、主信号フレームに付加するタグは、プロバイダを識別するものであったが、制御フレームに付加するタグは加入者側エッジL2SW20自身を識別するものとなる。ただし、加入者側エッジL2SW20の動作としては、テーブルからタグを引いて付加するにすぎない。なお、ETHER-TYPEが制御フレーム（例えば、0x8863）であれば、このタグを付加するというテーブル（付加するタグは、セッション管理サーバが加入者側エッジL2SWを識別できるID値）を持っていることになる。

【0204】そして、セッション管理サーバでは、受信フレームの送信元MACアドレス（ユーザ端末装置10のMACアドレス）でユーザのセッションを管理し、タグでどの加入者側エッジL2SW20配下であるかを把握することができる。なお、プロバイダRadiusサーバ52との通信はこの場合、セッション管理サーバがRadiusクライアントとして直接プロバイダRadiusサーバ52と行うことになる。

【0205】これはプロバイダから見て単一のRadiusクライアントと通信することには変わりはない。図51及び図52にセッション管理サーバの動作による接続イメージを示す。図52に示すように主信号フレームの流れについては変更はない。

【0206】また、図53に加入者側エッジL2SWの機能ブロック図を示す。図54は動作シーケンスを示す図である。なお、ユーザ端末装置10に搭載する機能や、プロバイダ側エッジL2SW51及びプロバイダ側の他装置に関しても変更はない。

【0207】以上説明したように、本発明により、加入者側エッジL2SW20は、主信号フレームも制御フレームもハード的に転送するだけなので、処理負荷が大幅に軽減される。またセッション管理は一箇所に集中することになるが、専用機器（サーバ）で処理するため、処理増大にともなうCPUやメモリのアップグレードは容易である。あるいは分散装置等を用いてセッション管理を複数サーバに分散させることも可能である。

【0208】次にセッション管理サーバの他の制御について説明する。セッション管理サーバは、ユーザ認証完了後にARPリレーテーブルを作成し、ユーザ端末装置10から送信されたARP Requestは加入者側エッジL2SWにてタグを付加してセッション管理サーバに転送する（ETHER TYPE=0x0806からARPであることを判別して、ハードウェア処理でタグを付加して転送する）。このタグはARPフレームを識別するタグをアクセス網6内で規定したものを用いる。

【0209】アクセス網6内では、このタグが付加されたフレームは、GVRP等公知の管理プロトコルにより、宛先不明の場合すなわちARP Request（ブロードキャスト）が不用意なフラディングが行われることなく、

セッション管理サーバに転送されるよう設定しておく。

【0210】そして、セッション管理サーバは、ARP Requestを受信し、ARPリレーテーブルにヒットした場合は、送信元ユーザに代理でARP Replyを返したり、または、ブロードキャストをユニキャストに変換して該当端末にのみ転送する。これによりユーザの秘匿性を確保しつつ、IPoEでの通信が可能となる。図55はセッション管理サーバの動作を示す図であり、図56、57は動作シーケンスを示す図である。

【0211】次に従来方式による接続先切り替え通信も収容する場合について説明する。ユーザ端末装置10が接続された加入者側エッジL2SW20において、PPPoEフレーム（ETHER-TYPE 0x8864）をCPUに回して処理する際に、PPP-PROTOCOL値が0x0021すなわちIPパケットをカプセル化したフレームであった場合には、MAC-VIDテーブルを参照して、接続先プロバイダのタグを抽出し（エントリにない場合は廃棄）、デカプセル化して、かつタグを付加したIPoEフレームとしてアクセス網6に転送する。

【0212】アクセス網6内のコアL2SW40及びプロバイダ側エッジL2SW30の動作及び他のプロバイダ側設備に変更は必要ない。そしてプロバイダからの下りフレームは、加入者側エッジL2SW20において、再びカプセル化を行ってユーザに転送する。

【0213】なお、本発明の動作は実際にはB-RAS同等の仮想ルータ機能を行うものである。すなわち、ユーザ端末装置10から受信したIP over PPP over Ethernet フレームをデカプセル化してアクセス網6に転送する際に、送信元MACアドレスは自L2SWのMACアドレス、宛先MACアドレスをプロバイダエッジルータのMACアドレスに付け替え、下りフレーム（宛先MACアドレスが自L2SW宛て）はCPUに回して転送先ユーザを決定し、宛先MACアドレスを該当ユーザ端末装置10のMACアドレス、送信元MACアドレスを自L2SWのMACアドレスに付け替えて転送する。

【0214】このような動作はソフトウェア処理が前提となるが、あくまで本発明の通信システム1において従来方式を収容するための手段であり、本発明のユーザ端末装置10と通信を行う場合は、主信号フレームはハードウェアによる高速処理を行うことに変わりはない。また上記のような動作をソフトウェア処理により行うことで、従来技術の内容を付加機能として組み込むことは容易である。

【0215】図58は本発明の動作を付加した場合の接続イメージ（ユーザ端末装置からIP over PPP over Ethernetで送出された場合）を示す。また、図59に本発明の方式と従来方式の場合の加入者側エッジL2SW内部でのIPデータの流れを示す。

【0216】次に本発明の通信接続プログラムについて

説明する。本発明であるユーザ端末装置10の処理機能は、通信接続プログラムとして、クライアントコンピュータによって実現することができる。その場合、本発明のクライアントに相当する装置が有すべき機能の処理内容を記述したクライアントプログラムが提供される。

【0217】そして、上記のようなコンピュータプログラムは、半導体メモリや磁気記録媒体などの記録媒体に記述させることができる。これにより、市場に流通させる場合に、CD-ROMやフレキシブルディスク等の可搬型記録媒体にプログラムを格納して流通させたり、ネットワークを介して接続されたコンピュータの記憶装置に格納しておき、ネットワークを通じて他のコンピュータに転送することもできる。また、コンピュータで実行する際には、コンピュータ内のハードディスク装置等にプログラムを格納しておき、メインメモリにロードして実行する。

【0218】次に本発明の通信システム1の変形例として、加入者側/コア（アクセス網）側/xSP側が一体となったL2SWを用いた場合のシステムについて説明する。

【0219】図60は一体型のL2SWを含む通信システムを示す図である。通信システム1aは、ユーザ端末装置10、通信管理サーバ61、加入者側/コア（アクセス網）側/xSP側が一体となったL2SW70、xSPから構成される。

【0220】一体型のスイッチを実現するためには、各ポートの属性を明確化し、加入者側ポートならば（送信元）MACアドレスからMAC-VIDテーブルを引き、コア（アクセス網）側であれば、タグからVIDを認識し、xSP側であれば入力ポートからポートVIDテーブルを引くという動作が必要となる。

【0221】そこで、上述のポート属性テーブルTdに変更を加え（図61に加入者側のポート属性テーブル、図62にxSP側のポート属性テーブルを示す）、テーブルにポート属性というパラメータを追加し、その設定によって、そのポートが加入者側なのかxSP側なのかコア（アクセス網）側なのかを設定するようにする。

【0222】例えば、コマンドラインで、#configure port 1 user、#configure port 5 coreなどと設定すると、各ポートがそれぞれの側に対応した設定になるようにする（VIDフィールドに関しては後述）。

【0223】そして、その他のパラメータ、すなわち受信フレーム（入力時に受け入れるフレーム）、ブロードキャストフィルタリング（ブロードキャストフレームやフラディング時にそのポートより出力するかフィルタリングするか）及びタグ挿抜（タグを付けて出力するか）は、ポート属性値よりデフォルト値（例えば、加入者側であれば、受信フレームは「PPPoE、IP、ARP」、ブロードキャストフィルタリングは「ON」、タグ挿抜は

「Untag」）が自動的に設定されるように変更する（つまり、ポート属性テーブルで、受信フレーム/ブロードキャストフィルタリング/タグ挿抜のそれぞれの値を逐一設定することを回避する）。

【0224】また、xSP側のL2SWのポート属性テーブルの設定値には、（VIDを静的に設定するため）VID値も同時に設定する。例えば、configure port 7 xspvid 12と設定すると、ポート7をxSP側設定とし、VIDが12となる。

【0225】一方、図1の送信処理手段で参照されるポートVIDテーブルは、本ユーザ設定値より登録され、主信号フレームはポートVIDテーブルにより、VIDが識別され、VIDごとのフォーワーディングテーブル（アドレス学習により自動生成）により転送される。コア側及びユーザ側のVIDは不定な（接続先毎に変わる）ので設定はしない。

【0226】そして、加入者側とxSP側が一体となったL2SWでは、フレーム入力時にポート属性テーブルから受信可能なETHER TYPEをチェックするとともに、ポート属性テーブルから主信号フレームのVIDを判断する。以降フォーワーディング、出力処理は変わらない。なお、図63に一体型のL2SWのブロック図を、図64に動作フローチャートを示す。

【0227】（付記1） ユーザからは、IPoEで主信号フレームを送受信し、前記ユーザでは、レイヤ2レベルで前記主信号フレームと区別可能な制御フレームによって、接続先の指定、ユーザ認証及びIPアドレス割り当ての処理を含む制御を行い、アクセス網にとっては、接続先仮想閉域網を識別して、送信元MACアドレスと、前記接続先仮想閉域網とをマッピングし、前記アクセス網では、MACブリッジングによってレイヤ2レベルの転送を行うことを特徴とする通信方法。

【0228】（付記2） アクセス網と、認証フェーズ時に、制御フレームを用いて、接続先の指定、ユーザ認証及びIPアドレス割り当ての処理を含む制御を行うユーザ側セッション管理手段と、通信フェーズ時に、カプセル化しない主信号フレームを送受信する主信号送受信手段と、から構成されて仮想閉域網に対するレイヤ2での接続を行うユーザ端末装置と、を有することを特徴とする通信システム。

【0229】（付記3） 前記ユーザ側セッション管理手段は、通信フェーズ時に、接続性確認フレームを定期的に送信することを特徴とする付記2記載の通信システム。

（付記4） 前記ユーザ側セッション管理手段は、主信号フレームの送受信を監視し、ユーザ設定可能な一定時間に、主信号フレームの通信が行われない場合は、自動的に接続を終了させることを特徴とする付記2記載の通信システム。

【0230】（付記5） 前記制御フレームの受信時に

は、シグナリング制御を行う網側セッション管理手段と、ユーザから転送された主信号フレームの受信時には、仮想閉域網を一意に示すタグを付加して転送し、前記接続先から転送された主信号フレームの受信時には、前記タグを外して前記ユーザ端末装置側へ転送する転送制御手段と、から構成される加入者側エッジスイッチ装置をさらに有することを特徴とする付記2記載の通信システム。

【0231】(付記6) 前記網側セッション管理手段は、前記レイヤ2アドレスとユーザとのセッション対応を示すテーブルを用いて、ソフトウェア処理でシグナリング制御を行い、前記転送制御手段は、前記レイヤ2アドレスと前記接続先毎の前記タグとの対応を示すテーブルと、前記接続先毎に独立したフォワーディング情報を示すテーブルと、各ポートの属性を示すテーブルとを用いて、ハードウェア処理で、主信号フレームの転送を行うことを特徴とする付記5記載の通信システム。

【0232】(付記7) 前記転送制御手段は、各ポートの属性を示す前記テーブルにもとづいて、入力フレームの受け入れ可否の判断、出力フレームのタグ挿抜またはブロードキャストフィルタリングのON/OFFの判断、ユニキャストのフラッディングのフィルタリング処理を行うことを特徴とする付記5記載の通信システム。

【0233】(付記8) 前記転送制御手段は、カプセル化された主信号を受信した場合には、デカプセル化した後に、前記タグを付加して転送することを特徴とする付記5記載の通信システム。

【0234】(付記9) 複数の前記接続先と同時接続する場合、前記転送制御手段は、前記ユーザ端末装置及び前記接続先それぞれのレイヤ2アドレスにより、接続先を一意に識別することを特徴とする付記5記載の通信システム。

【0235】(付記10) 複数の前記接続先と同時接続する場合、前記転送制御手段は、前記ユーザ端末装置のレイヤ2アドレス及び前記接続先のレイヤ3アドレスにより、接続先を一意に識別することを特徴とする付記5記載の通信システム。

【0236】(付記11) 前記網側セッション管理手段は、シグナリング制御時に前記タグを前記ユーザ端末装置へ配布し、複数の前記接続先と同時接続する場合、前記主信号送受信手段は、前記タグを付加した主信号フレームを前記加入者側エッジスイッチ装置に送信して、前記加入者側エッジスイッチ装置が接続先を一意に識別することを特徴とする付記5記載の通信システム。

【0237】(付記12) 前記タグと出力ポートとが対応して、前記タグを外して前記接続先へ主信号フレームを出力する出力処理手段と、入力ポートより前記接続先を判断し、前記タグを付加して前記ユーザ端末装置側へ送信する送信処理手段と、から構成される接続先側エッジスイッチ装置をさらに有することを特徴とする付記

2記載の通信システム。

【0238】(付記13) 前記加入者側エッジスイッチ装置及び前記接続先側エッジスイッチ装置は、レイヤ2アドレスとレイヤ3アドレスの対応を示すテーブルを生成し、送信元装置から宛先装置のレイヤ2アドレスを求めるリクエストがあった場合、前記テーブルにもとづき、前記宛先装置の代理応答を行って、前記レイヤ2アドレスを返信して、アドレス解決制御を行うアドレス解決手段をさらに有することを特徴とする付記2記載の通信システム。

【0239】(付記14) 前記アドレス解決手段は、前記送信元装置のレイヤ2アドレスを前記宛先装置へユニキャスト転送することを特徴とする付記13記載の通信システム。

【0240】(付記15) 前記ユーザ端末装置からの認証情報の集約、前記認証情報の前記接続先への転送、前記接続先で認証制御された結果を示す認証メッセージの前記ユーザ端末装置への転送、を含む認証に関する一元管理処理を行う通信管理サーバをさらに有することを特徴とする付記2記載の通信システム。

【0241】(付記16) 前記網側セッション管理手段を前記通信管理サーバに、前記転送制御手段を前記加入者側エッジスイッチ装置に持たせて、前記制御フレームの処理と、前記主信号フレームの処理とを装置的に分離することを特徴とする付記15記載の通信システム。

【0242】(付記17) 前記加入者側エッジスイッチ装置は、前記ユーザ端末装置からの前記制御フレームに、自配下にユーザが存在することを示すタグを付加して、ハードウェア処理で前記通信管理サーバに送信し、前記通信管理サーバでは、認証成功時に、前記加入者側エッジスイッチ装置に、接続先を識別するためのテーブルを遠隔設定することを特徴とする付記15記載の通信システム。

【0243】(付記18) 前記通信管理サーバは、レイヤ2アドレスとレイヤ3アドレスの対応を示すテーブルを生成し、前記加入者側エッジスイッチ装置は、宛先装置のレイヤ2アドレスを求めるリクエストを、ハードウェア処理で前記通信管理サーバに送信して、アドレス解決制御を行うことを特徴とする付記15記載の通信システム。

【0244】(付記19) 認証フェーズ時に、制御フレームを用いて、接続先の指定、ユーザ認証及びIPアドレス割り当ての処理を含む制御を行うユーザ側セッション管理手段と、通信フェーズ時に、カプセル化しない主信号フレームを送受信する主信号送受信手段と、を有することを特徴とする、仮想閉域網に対するレイヤ2での接続を行うユーザ端末装置。

【0245】(付記20) 前記ユーザ側セッション管理手段は、通信フェーズ時に、接続性確認フレームを定期的に送信することを特徴とする付記19記載のユーザ

端末装置。

【0246】(付記21) 前記ユーザ側セッション管理手段は、主信号フレームの送受信を監視し、ユーザ設定可能な一定時間に、主信号フレームの通信が行われない場合は、自動的に接続を終了させることを特徴とする付記19記載のユーザ端末装置。

【0247】(付記22) 複数の前記接続先と同時接続する場合、前記主信号送受信手段は、ネットワーク側から配布された接続先を一意に示すタグを付加した主信号フレームを送信することを特徴とする付記19記載のユーザ端末装置。

【0248】(付記23) 制御フレームの受信時には、シグナリング制御を行う網側セッション管理手段と、ユーザから転送された主信号フレームの受信時には、仮想閉域網を一意に示すタグを付加して転送し、接続先から転送された主信号フレームの受信時には、前記タグを外してユーザ端末装置側へ転送する転送制御手段と、を有することを特徴とする加入者側エッジスイッチ装置。

【0249】(付記24) 前記網側セッション管理手段は、前記レイヤ2アドレスとユーザとのセッション対応を示すテーブルを用いて、ソフトウェア処理でシグナリング制御を行い、前記転送制御手段は、前記レイヤ2アドレスと前記接続先毎の前記タグとの対応を示すテーブルと、前記接続先毎に独立したフォワーディング情報を示すテーブルと、各ポートの属性を示すテーブルとを用いて、ハードウェア処理で、主信号フレームの転送を行うことを特徴とする付記23記載の加入者側エッジスイッチ装置。

【0250】(付記25) 前記転送制御手段は、各ポートの属性を示す前記テーブルにもとづいて、入力フレームの受け入れ可否の判断、出力フレームのタグ挿抜またはブロードキャストフィルタリングのON/OFFの判断、ユニキャストのフラッディングのフィルタリング処理を行うことを特徴とする付記23記載の加入者側エッジスイッチ装置。

【0251】(付記26) レイヤ2アドレスとレイヤ3アドレスの対応を示すテーブルを生成し、送信元装置から宛先装置のレイヤ2アドレスを求めるリクエストがあった場合、前記テーブルにもとづき、前記宛先装置の代理応答を行って、前記レイヤ2アドレスを返信して、アドレス解決制御を行うアドレス解決手段をさらに有することを特徴とする付記23記載の加入者側エッジスイッチ装置。

【0252】(付記27) 前記アドレス解決手段は、前記送信元装置のレイヤ2アドレスを前記宛先装置へユニキャスト転送することを特徴とする付記26記載の加入者側エッジスイッチ装置。

【0253】(付記28) 複数の前記接続先と同時接続する場合、前記転送制御手段は、ユーザ端末装置及び

前記接続先それぞれのレイヤ2アドレスにより、接続先を一意に識別することを特徴とする付記23記載の加入者側エッジスイッチ装置。

【0254】(付記29) 複数の前記接続先と同時接続する場合、前記転送制御手段は、ユーザ端末装置のレイヤ2アドレス及び前記接続先のレイヤ3アドレスにより、接続先を一意に識別することを特徴とする付記23記載の加入者側エッジスイッチ装置。

【0255】(付記30) 前記網側セッション管理手段は、ユーザが複数の前記接続先と同時接続する際には、シグナリング制御時に前記タグを前記ユーザ端末装置へ配布することを特徴とする付記23記載の加入者側エッジスイッチ装置。

【0256】(付記31) 前記転送制御手段は、カプセル化された主信号を受信した場合には、デカプセル化した後に、前記タグを付加して転送することを特徴とする付記23記載の加入者側エッジスイッチ装置。

【0257】(付記32) タグと出力ポートとが対応して、前記タグを外して接続先へ主信号フレームを出力する出力処理手段と、入力ポートより前記接続先を判断し、前記タグを付加してユーザ端末装置側へ送信する送信処理手段と、を有することを特徴とする接続先側エッジスイッチ装置。

【0258】(付記33) レイヤ2アドレスとレイヤ3アドレスの対応を示すテーブルを生成し、送信元装置から宛先装置のレイヤ2アドレスを求めるリクエストがあった場合、前記テーブルにもとづき、前記宛先装置の代理応答を行って、前記レイヤ2アドレスを返信して、アドレス解決制御を行うアドレス解決手段をさらに有することを特徴とする付記32記載の接続先側エッジスイッチ装置。

【0259】(付記34) 前記アドレス解決手段は、前記送信元装置のレイヤ2アドレスを前記宛先装置へユニキャスト転送することを特徴とする付記33記載の接続先側エッジスイッチ装置。

【0260】(付記35) 接続先を一意に示すタグを参照するタグ参照手段と、レイヤ2で主信号フレームの転送を行うコアシッチング転送手段と、を有することを特徴とするコアシッチ装置。

【0261】(付記36) 認証サーバとして動作する際、ユーザ端末装置からの認証情報の集約、前記認証情報の接続先への転送、前記接続先で認証制御された結果を示す認証メッセージの前記ユーザ端末装置への転送、を含む認証に関する一元管理処理を行う認証制御手段と、セッション管理サーバとして動作する際、制御フレームの受信時に、シグナリング制御を行うセッション管理手段と、を有することを特徴とする通信管理サーバ。

【0262】(付記37) 前記認証制御手段と前記ユーザ端末装置間で、認証タグが付加された認証情報により、前記認証情報を含むフレームであることを認識して

通信を行うことを特徴とする付記36記載の通信管理サーバ。

【0263】(付記38) 前記セッション管理手段は、加入者側エッジスイッチ装置から送信された、自配下にユーザが存在することを示すタグが付加された制御フレームを受信し、認証成功時には、前記加入者側エッジスイッチ装置に、接続先を識別するためのテーブルを遠隔設定することを特徴とする付記36記載の通信管理サーバ。

【0264】(付記39) 前記セッション管理手段は、レイヤ2アドレスとレイヤ3アドレスの対応を示すテーブルを生成し、前記加入者側エッジスイッチ装置は、宛先装置のレイヤ2アドレスを求めるリクエストを、ハードウェア処理で前記通信管理サーバに送信して、アドレス解決制御を行うことを特徴とする付記36記載の通信管理サーバ。

【0265】(付記40) ユーザ端末装置側に装備され、仮想閉域網に対するレイヤ2での接続を行う通信接続プログラムにおいて、コンピュータに、認証フェーズ時に、制御フレームを用いて、接続先の指定、ユーザ認証及びIPアドレス割り当ての処理を含む制御を行い、通信フェーズ時に、カプセル化しない主信号フレームを送受信する、処理を実行させることを特徴とする通信接続プログラム。

【0266】(付記41) 通信フェーズ時に、接続性確認フレームを定期的に送信する処理をさらに含むことを特徴とする付記40記載の通信接続プログラム。(付記42) 主信号フレームの送受信を監視し、ユーザ設定可能な一定時間に、主信号フレームの通信が行われない場合は、自動的に接続を終了させる処理をさらに含むことを特徴とする付記40記載の通信接続プログラム。

【0267】(付記43) 複数の前記接続先と同時に接続する場合、ネットワーク側から配布された接続先を一意に示すタグを付加した主信号フレームを送信する処理をさらに含むことを特徴とする付記40記載の通信接続プログラム。

【0268】
【発明の効果】以上説明したように、本発明の通信方法は、ユーザからは、IPoEでの主信号フレームの送受信及び制御フレームによって、接続先の指定、ユーザ認証及びIPアドレス割り当ての処理を含む制御を行い、アクセス網にとっては、接続先仮想閉域網を識別して、送信元MACアドレスと、接続先仮想閉域網とをマッピングして、MACブリッジングによってレイヤ2レベルの転送を行うこととした。これにより、レイヤ2レベルでの高速通信可能なVPNシステムを構築することができるので、ユーザは接続先を任意に切り替えて、効率よくサービスを受けることができ、ユーザとプロバイダ間での通信サービスの品質及び利便性の向上を図ることが可能になる。

【0269】また、本発明の通信システムは、レイヤ2での通信接続を行うユーザ端末装置で、認証フェーズ時に、制御フレームを用いて、接続先の指定、ユーザ認証及びIPアドレス割り当ての処理を含む制御を行い、通信フェーズ時には、カプセル化しない主信号フレームを送受信する処理を行い、また、ユーザ側/接続側のエッジスイッチ装置では、主信号フレームに対してタグの挿入を行って、レイヤ2レベルでの転送を行う構成とした。これにより、レイヤ2レベルでの高速通信可能なVPNシステムを構築することができるので、ユーザは接続先を任意に切り替えて、効率よくサービスを受けることができ、ユーザとプロバイダ間での通信サービスの品質及び利便性の向上を図ることが可能になる。

【0270】さらに、本発明のユーザ端末装置は、認証フェーズ時に、制御フレームを用いて、接続先の指定、ユーザ認証及びIPアドレス割り当ての処理を含む制御を行い、通信フェーズ時には、カプセル化しない主信号フレームを送受信する処理を行う構成とした。これにより、レイヤ2レベルでの高速通信可能なVPNシステムに対して、ユーザは接続先を任意に切り替えて、効率よくサービスを受けることができ、ユーザとプロバイダ間での通信サービスの品質及び利便性の向上を図ることが可能になる。

【0271】また、本発明の通信接続プログラムは、制御フレームを用いて、接続先の指定、ユーザ認証及びIPアドレス割り当ての処理を含む制御を行い、通信フェーズ時には、カプセル化しない主信号フレームを送受信する処理を行うこととした。これにより、レイヤ2レベルでの高速通信可能なVPNシステムに対して、ユーザは接続先を任意に切り替えて、効率よくサービスを受けることができ、ユーザとプロバイダ間での通信サービスの品質及び利便性の向上を図ることが可能になる。

【図面の簡単な説明】

【図1】本発明の通信システムの原理図である。

【図2】フレーム構成を示す図である。(A)は改正前、(B)は改正後、(C)はPPPoEでカプセル化した場合のフレーム構成を示している。

【図3】通信システムの構成例を示す図である。

【図4】主信号フレームのフォーマットを示す図である。

【図5】主信号フレームのフォーマットを示す図である。

【図6】認証フェーズ時のシーケンスを示す図である。

【図7】加入者側エッジL2SWが有するテーブルを示す図である。

【図8】加入者側エッジL2SWが有するテーブルを示す図である。

【図9】加入者側エッジL2SWが有するテーブルを示す図である。

【図10】加入者側エッジL2SWが有するテーブルを

示す図である。

【図11】加入者側エッジL2SWの動作概要を示す図である。

【図12】加入者側エッジL2SWのブロック構成を示す図である。

【図13】加入者側エッジL2SWの全体動作を示すフローチャートである。

【図14】加入者側エッジL2SWのPPPoEネゴシエーションの動作を示すフローチャートである。

【図15】加入者側エッジL2SWのフォワーディング処理／出力処理の動作を示すフローチャートである。

【図16】ユーザ端末装置の構成を示す図である。

【図17】従来のユーザ端末におけるプロトコルスタックを示す図である。

【図18】ユーザ側セッション管理テーブルを示す図である。

【図19】ルーティングテーブルを示す図である。

【図20】LCP Echo-Requestのフォーマット構成を示す図である。

【図21】LCP Terminate-Requestのフォーマット構成を示す図である。

【図22】ゲートウェイルータを用いたシステム例を示す図である。

【図23】ユーザ端末装置の動作を示すフローチャートである。

【図24】ARP Request及びReplyのフォーマットを示す図である。

【図25】一般のARPの動作を示す図である。

【図26】ARPリレーテーブルを示す図である。

【図27】Proxy ARPの動作を示す図である。

【図28】本発明のARPの制御を示す図である。

【図29】IPv6データフレームのフォーマットを示す図である。

【図30】本発明のARPの制御を示す図である。

【図31】動作シーケンスを示す図である。

【図32】動作シーケンスを示す図である。

【図33】IP通信フェーズ及び接続性確認処理を行うシーケンス図である。

【図34】IP通信フェーズ及び接続性確認処理を行うシーケンス図である。

【図35】プロバイダ側エッジL2SWが有するテーブルを示す図である。

【図36】プロバイダ側エッジL2SWのモデル図である。

【図37】プロバイダ側エッジL2SWのブロック構成を示す図である。

【図38】プロバイダ側エッジL2SWの動作を示すフローチャートである。

【図39】Proxy Radiusサーバの動作を説明する図である。

【図40】プロバイダ管理テーブルを示す図である。

【図41】動作シーケンスを示す図である。

【図42】複数同時接続時のセッション管理テーブルを示す図である。

【図43】複数同時接続のイメージ図である。

【図44】宛先MACアドレステーブルを示す図である。

【図45】複数マッチした場合の加入者側エッジL2SWの動作を示すフローチャートである。

【図46】複数マッチした場合のARPリレー処理を示すフローチャートである。

【図47】IPサブネットテーブルを示す図である。

【図48】複数マッチした場合の加入者側エッジL2SWの動作を示すフローチャートである。

【図49】加入者側エッジL2SWの動作を示すフローチャートである。

【図50】接続イメージを示す図である。

【図51】接続イメージを示す図である。

【図52】接続イメージを示す図である。

【図53】加入者側エッジL2SWのブロック構成を示す図である。

【図54】動作シーケンスを示す図である。

【図55】セッション管理サーバの動作を示す図である。

【図56】動作シーケンスを示す図である。

【図57】動作シーケンスを示す図である。

【図58】接続イメージを示す図である。

【図59】加入者側エッジL2SWのIPデータの流れを示す図である。

【図60】一体型のL2SWを含む通信システムを示す図である。

【図61】加入者側のポート属性テーブルを示す図である。

【図62】xSP側のポート属性テーブルを示す図である。

【図63】一体型のL2SWのブロック図である。

【図64】動作フローチャートを示す図である。

【図65】ユーザとプロバイダとの接続形態を示す図である。

【図66】PPPoEを利用した従来のネットワークシステムを示す図である。

【符号の説明】

1 通信システム

10 ユーザ端末装置

11 ユーザ側セッション管理手段

12 主信号送受信手段

20 加入者側エッジスイッチ装置

21 網側セッション管理手段

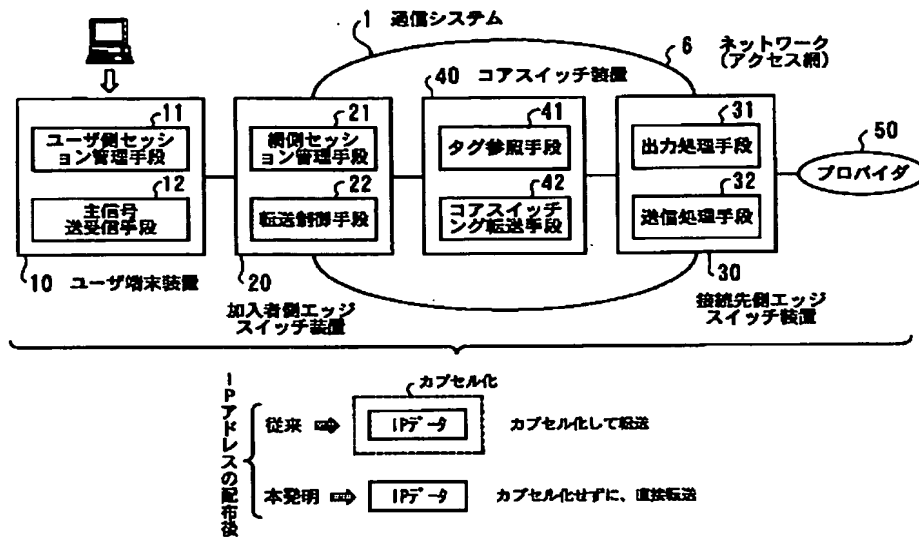
22 転送制御手段

30 接続先側エッジスイッチ装置

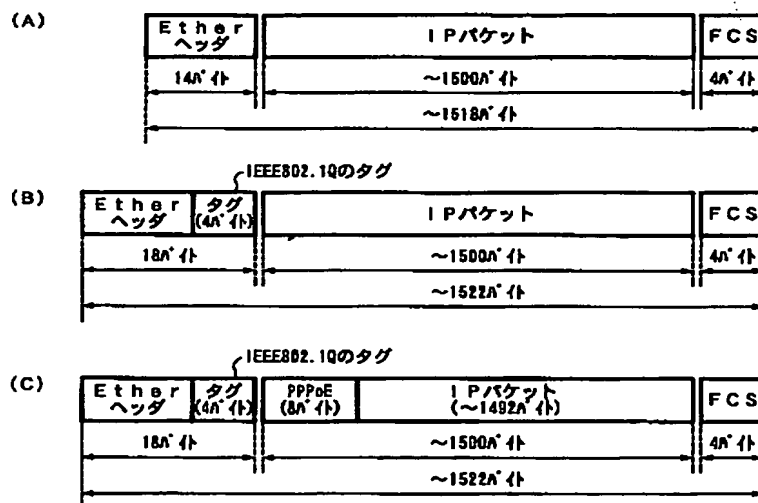
31 出力処理手段
32 送信処理手段
40 コアスイッチ装置
41 タグ参照手段

42 コアスイッチング転送手段
50 プロバイダ
6 アクセス網

【図1】



【図2】

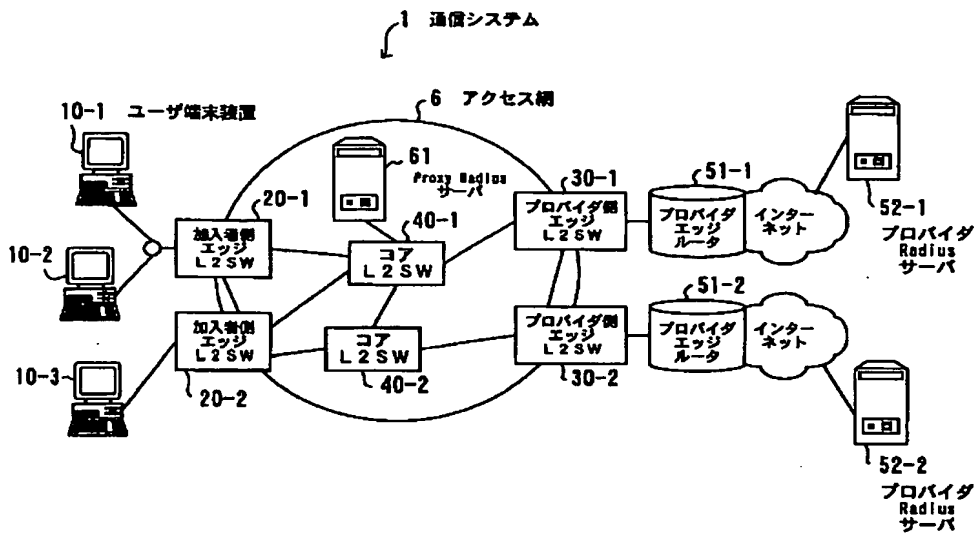


【図4】

0										31									
DESTINATION ADDR																			
DESTINATION ADDR										SOURCE ADDR									
SOURCE ADDR																			
ETHER TYPE(=0x0800)										VER		IHL		TOS					
TOTAL LENGTH										FLAGS		FRAGMENT OFFSET							
TTL				PROTOCOL						HEADER CHECKSUM									
SOURCE IP ADDR																			
DESTINATION IP ADDR																			
OPTIONS														PADDING					

1HL: Internet Header Length
TOS: Type Of Service
TTL: Time To Live

【図3】



【図5】

DESTINATION ADDR	
DESTINATION ADDR	SOURCE ADDR
SOURCE ADDR	
TPID(=0x8100)	PRI (0~7) VID(=1~4094)
ETHER TYPE(=0x0800)	IP PACKET...

TPID:Tag Protocol Identifier

PRI :Priority

CFI :Canonical Format Indicator

VID :VLAN Identifier

【図7】

T2a セッション管理テーブル

MAC アドレス	セッション ID	状態	ネゴシエーションパラメータ
A	0x1234	IP通信フェーズ	VLAN-ID=10, 割当IPアドレス=a, xSP-IPアドレス=X
B	0x5678	IP通信フェーズ	VLAN-ID=11, 割当IPアドレス=b, xSP-IPアドレス=y
C	0x7777	認証フェーズ	VLAN-ID=12 (IPアドレスはネゴシエーション中のため未設定)
D	0x8859	IP通信フェーズ	VLAN-ID=11, 割当IPアドレス=d, xSP-IPアドレス=y
----	----	----	----

【図8】

T2b MAC-VIDテーブル

MAC アドレス	セッション ID	VLAN-ID
A	0x1234	10
B	0x5678	11
D	0x8859	11
----	----	----

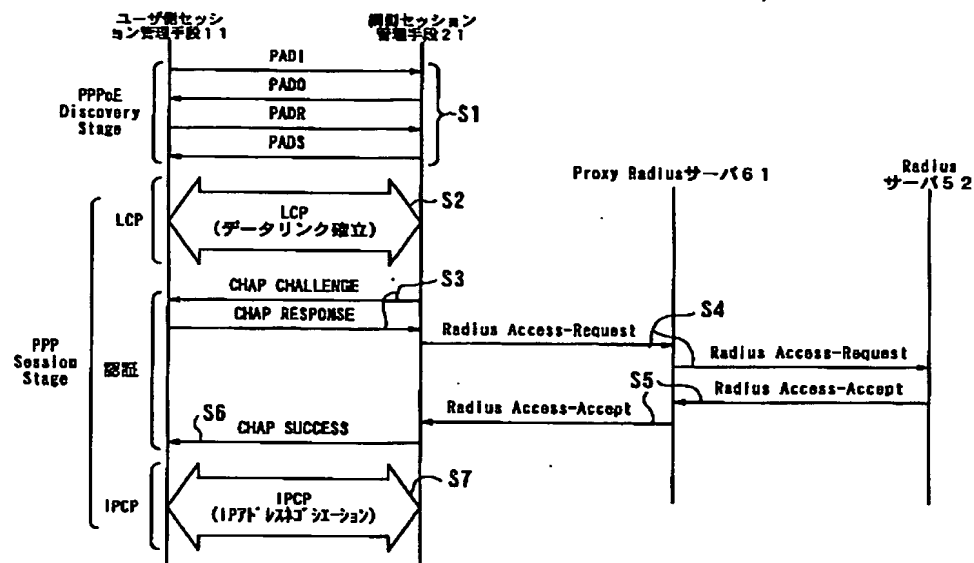
← Cは認証フェーズ中であるため未登録

【図10】

T2d ポート属性テーブル

ポート番号	受信フレーム	ブロードキャストフィルタリング	タグ挿抜
1	PPPoE, IP, ARP	ON	UnTag
2	PPPoE, IP, ARP	ON	UnTag
3	PPPoE, IP, ARP	ON	UnTag
4	PPPoE, IP, ARP	ON	UnTag
5	IEEE802.1Q, GVRP, STP	OFF	With Tag
6	IEEE802.1Q, GVRP, STP	OFF	With Tag
7	IEEE802.1Q, GVRP, STP	OFF	With Tag
----	----	----	----

【図6】

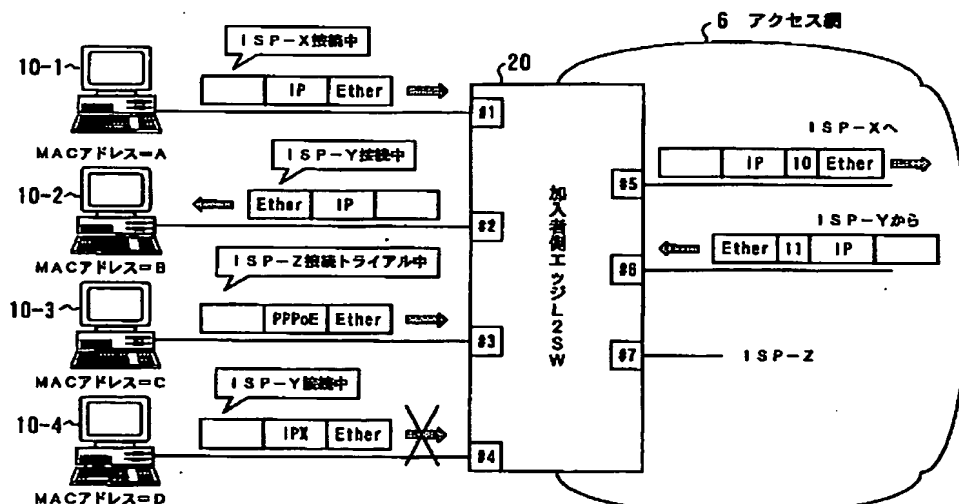


【図9】

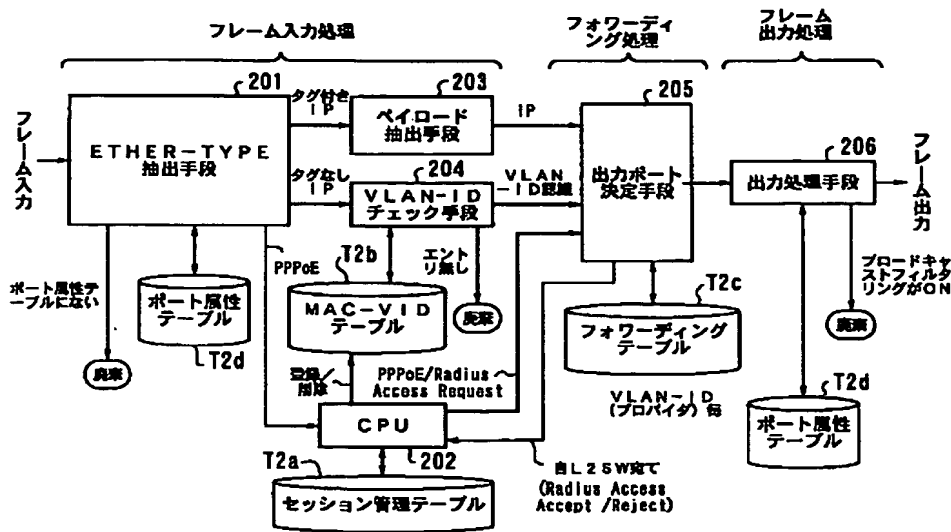
T2c フォワーディングテーブル

For VLAN-ID=10		For VLAN-ID=11		For VLAN-ID=12	
MAC アドレス	出力ポート	MAC アドレス	出力ポート	MAC アドレス	出力ポート
A	1	B	2	C	3
X	5	D	4	Z	7
---	---	Y	6	---	---

【図11】

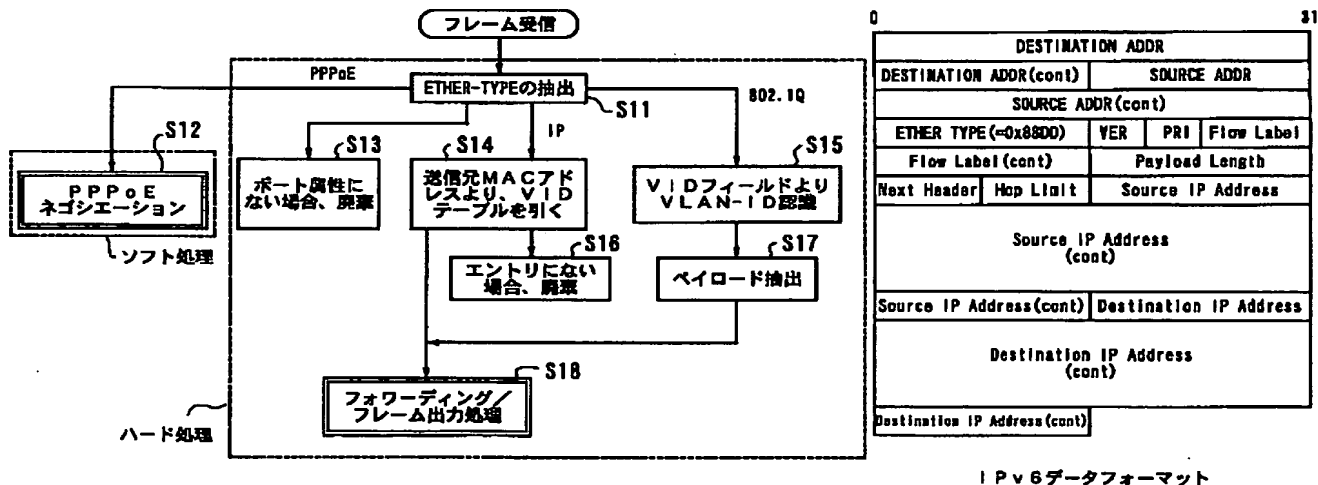


【図12】

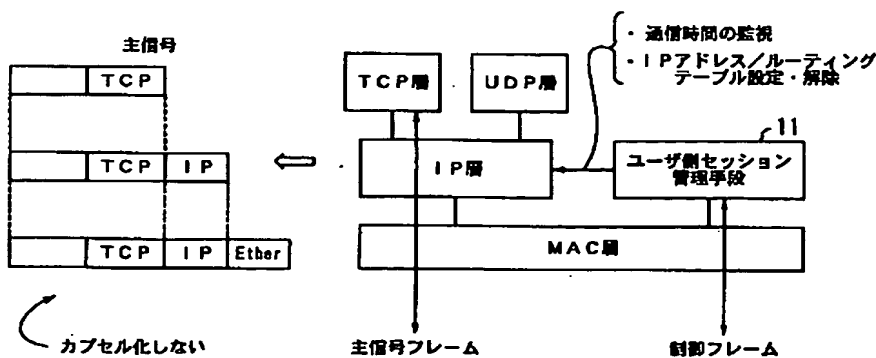


【図13】

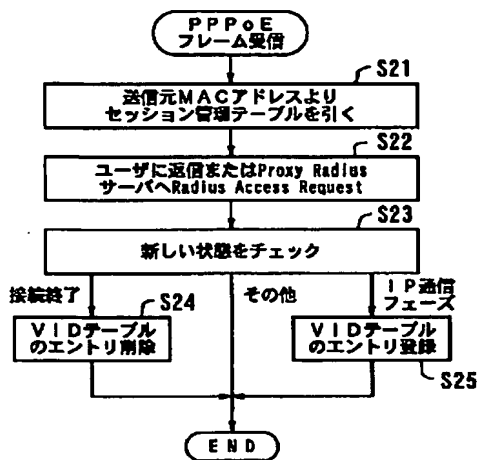
【図29】



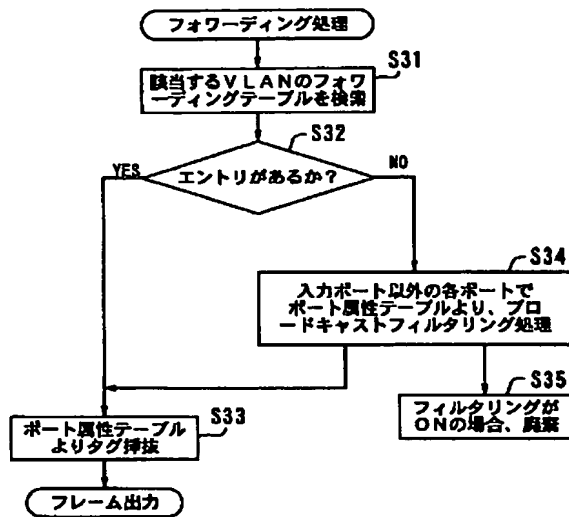
【図16】



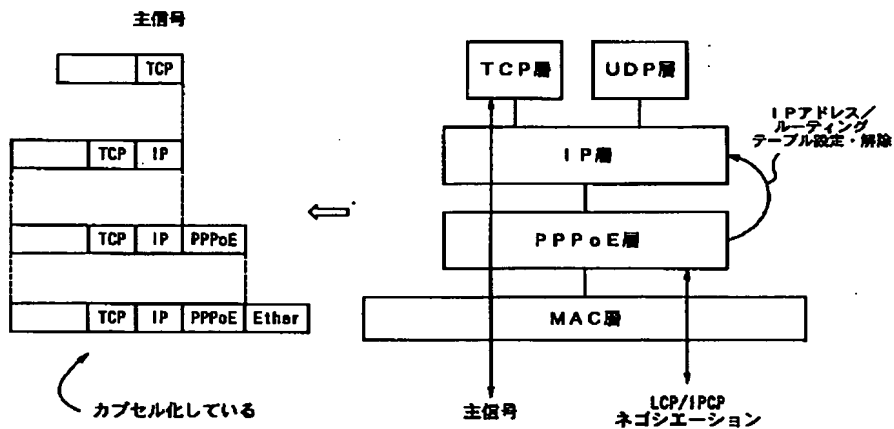
【図14】



【図15】



【図17】



【図18】

(接続前)

MAC アドレス	セッション ID	状態	ネゴシエーションパラメータ
?	0x0000	接続トライアル	ユーザID: ユーザ名@プロバイダ名、パスワード

接続先が一意に固定の場合は、
あらかじめ記憶させておくことも可能

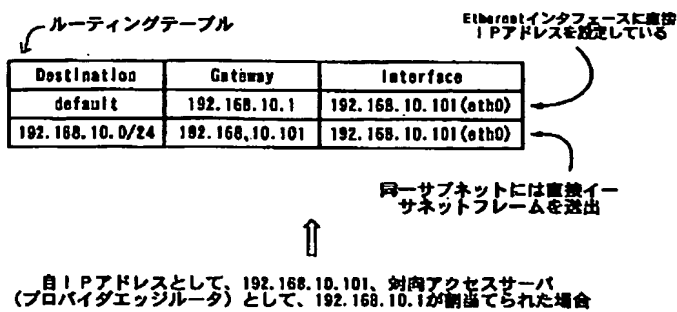
(接続後)

MAC アドレス	セッション ID	状態	ネゴシエーションパラメータ
M	0x1234	IP通信フェーズ	相対IPアドレス=a、プロバイダーIPアドレス=x

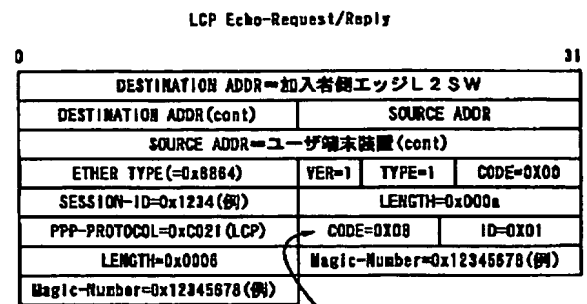
加入者側エッジL2SW
のMACアドレス

aを自EthernetインタフェースのIPアドレスに設定
xをデフォルトルートに設定

【図19】

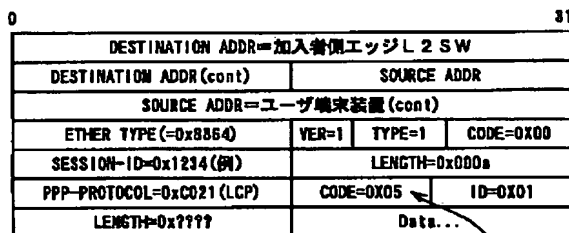


【図20】



(LCP Echo-Requestの受信端末は、CODE=0x09(Reply)
Magic-Numberを自端末設定値にして返信)

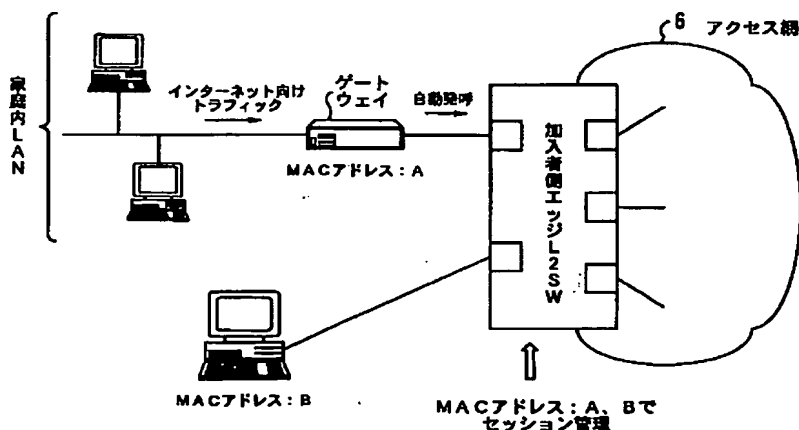
【図21】



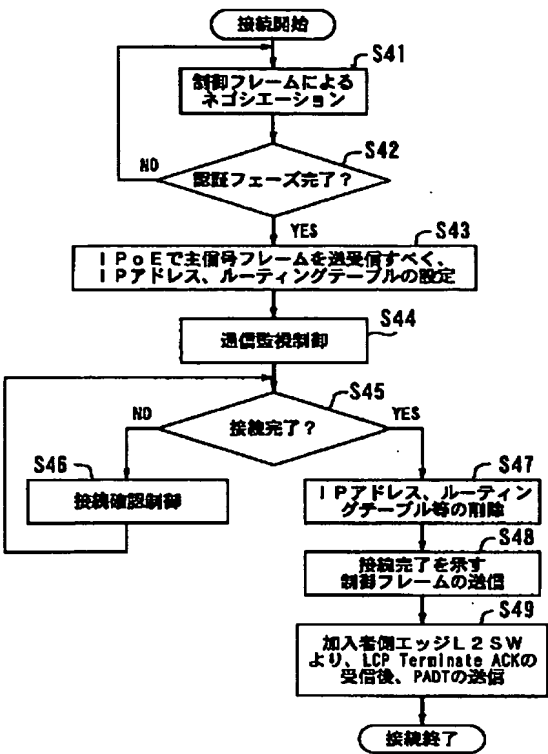
LCP Terminate-Request/Ack

(LCP Terminate-Requestの受信端末は、CODE=0x06(Ack)にして返信、Dataは切断理由等を示す)

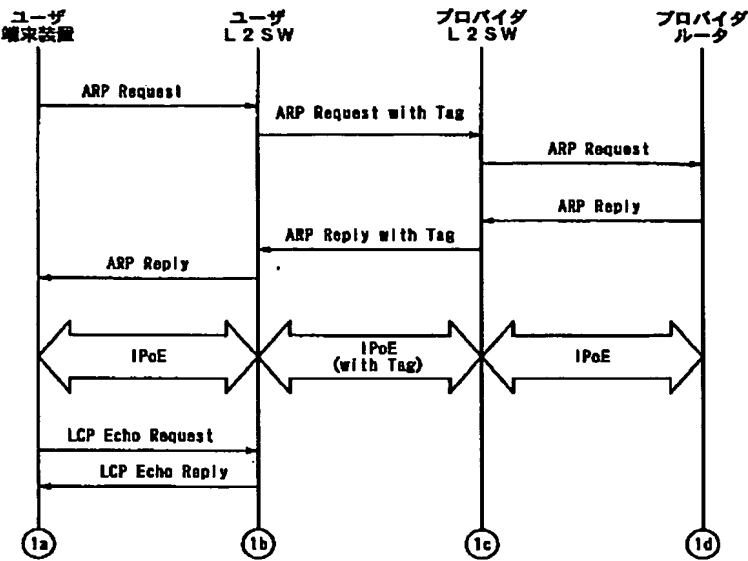
【図22】



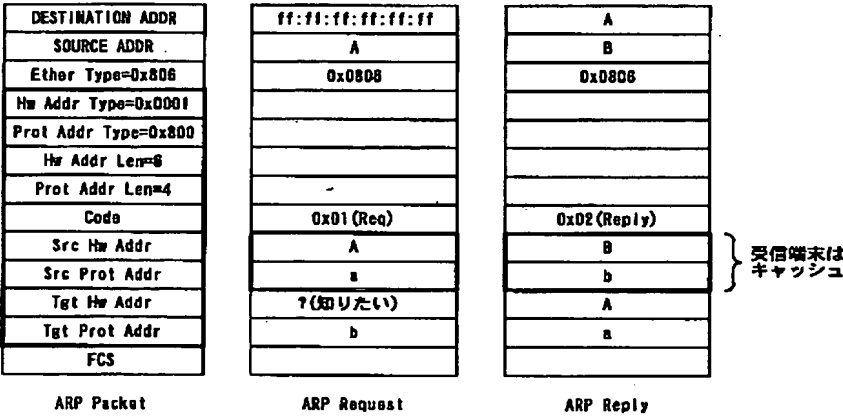
【図23】



【図33】



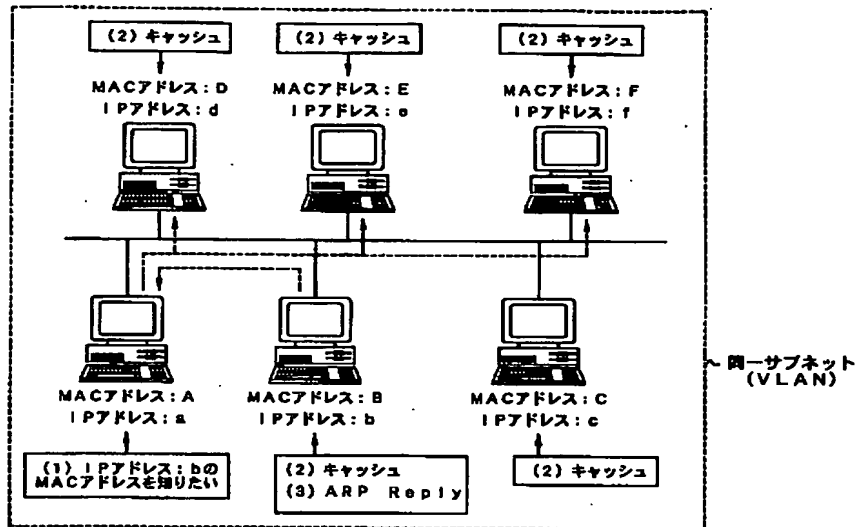
【図24】



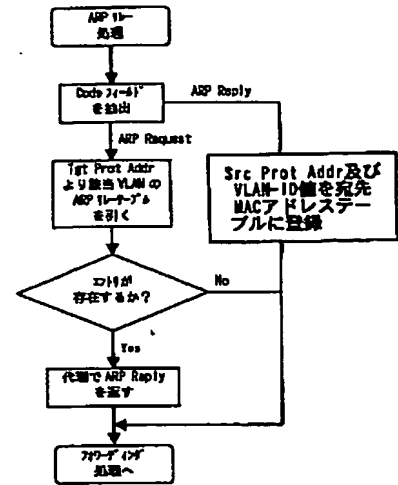
【図40】

プロバイダ名	VLAN-ID	プロバイダRadius サーバ情報
ISP-X	10	IPアドレス=x1
ISP-Y	11	IPアドレス=y1
ISP-Z	12	IPアドレス=z1

【図25】



【図46】



【図26】

セッション管理テーブル

MAC アドレス	セッション ID	状態	ネゴシエーションパラメータ
A	0x1234	IP 通信フェーズ	VLAN-ID=10、割当IPアドレス=a、xSP-IPアドレス=X
B	0x5678	IP 通信フェーズ	VLAN-ID=11、割当IPアドレス=b、xSP-IPアドレス=y
C	0x7777	認証フェーズ	VLAN-ID=12 (IPアドレスはネゴシエーション中のため未設定)
D	0x3859	IP 通信フェーズ	VLAN-ID=11、割当IPアドレス=d、xSP-IPアドレス=y
---	---	---	---

認証フェーズ
完了後

IPアドレス	MACアドレス	IPアドレス	MACアドレス	IPアドレス	MACアドレス
a	A	b	B		?
---	---	d	D	---	---
For VLAN-ID=10		For VLAN-ID=11		For VLAN-ID=12	

ARPリレーテーブル (VLAN-IDごとに独立)

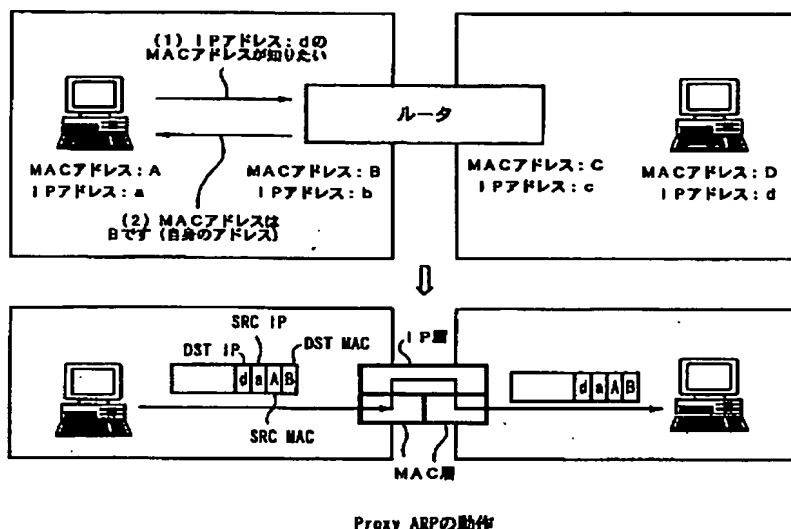
【図42】

MAC アドレス	セッション ID	状態	ネゴシエーションパラメータ
A	0x1234	IP 通信フェーズ	VLAN-ID=10、割当IPアドレス=a、xSP-IPアドレス=X
A	0x5678	IP 通信フェーズ	VLAN-ID=11、割当IPアドレス=b、xSP-IPアドレス=y
B	0x7777	認証フェーズ	VLAN-ID=12 (IPアドレスはネゴシエーション中のため未設定)
C	0x3859	IP 通信フェーズ	VLAN-ID=11、割当IPアドレス=d、xSP-IPアドレス=y
---	---	---	---

Aが複数同時接続中

ただし、送信元MACアドレス+セッションIDでセッションを一意に識別

【图27】

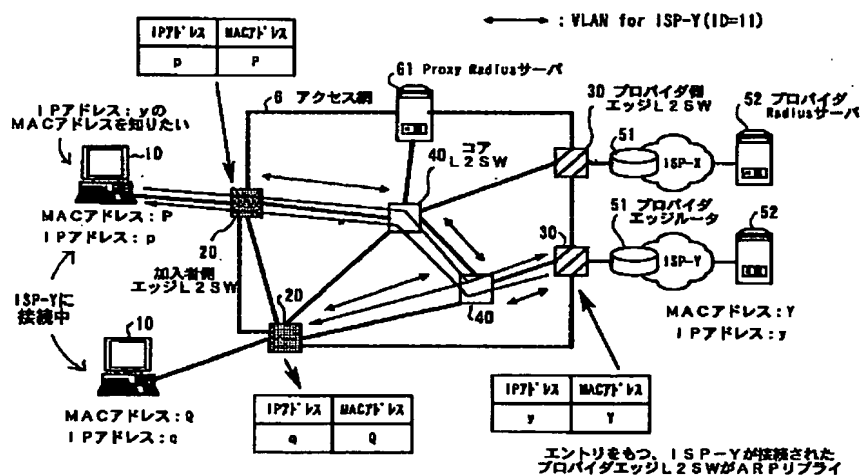


【图47】

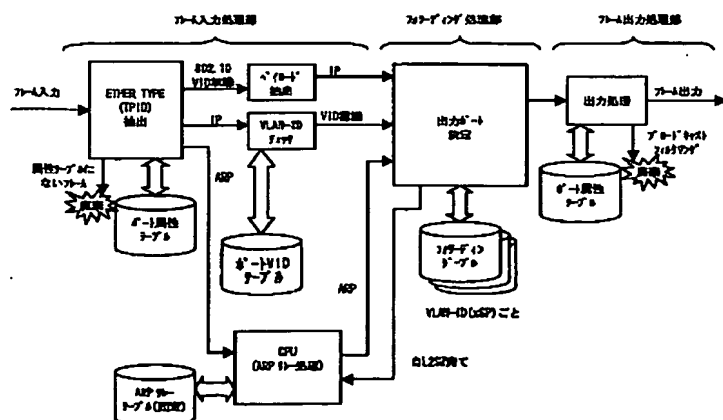
IPサブネット	VLAN-ID
xxx. xxx. xxx. 0/24	10
yyy. yyy. yyy. 0/24	11

IPサブネットテーブル

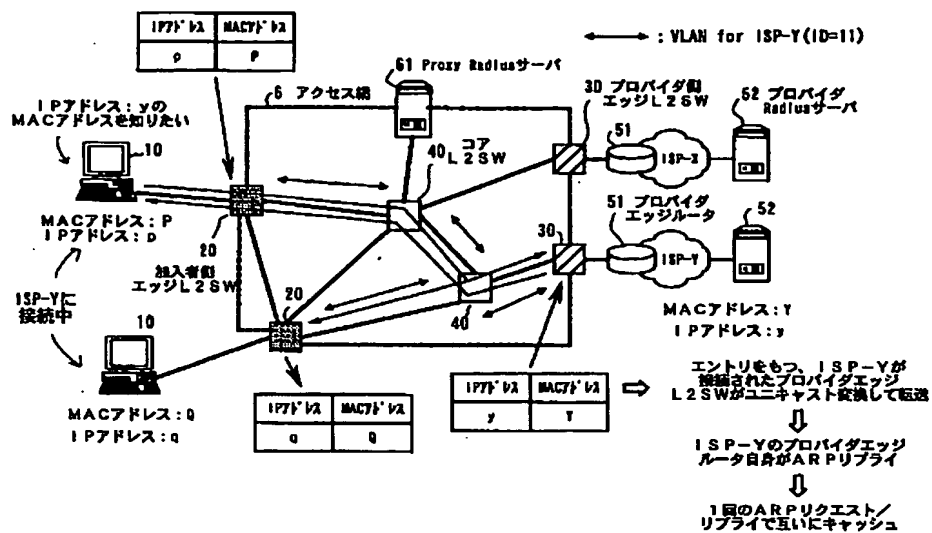
【图28】



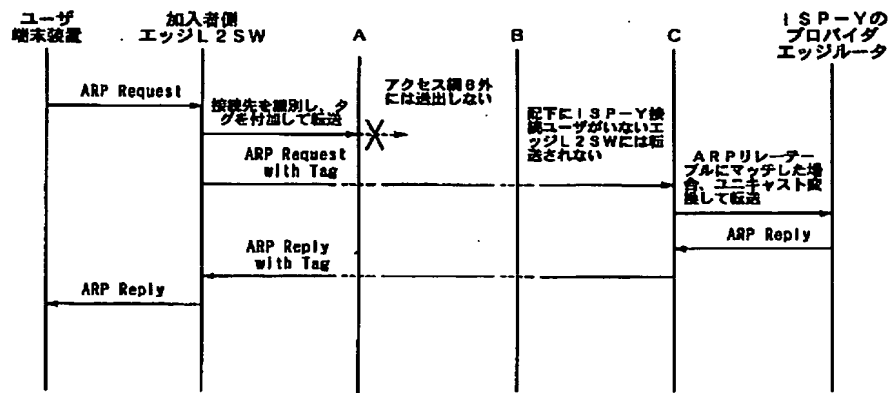
【図37】



【図30】

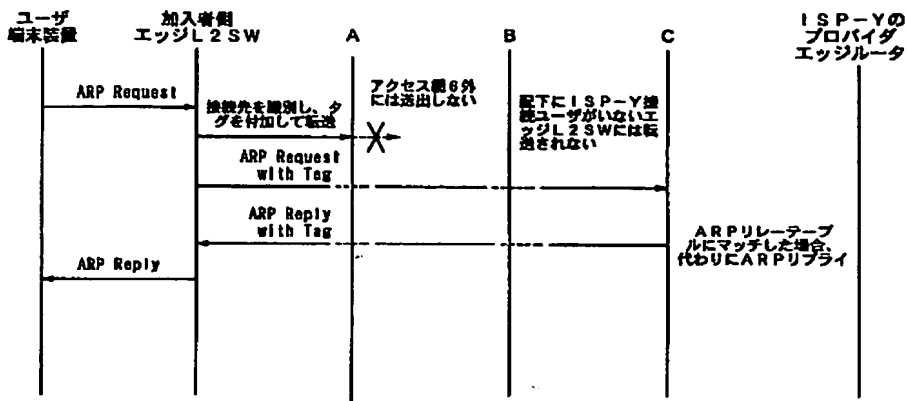


【図31】



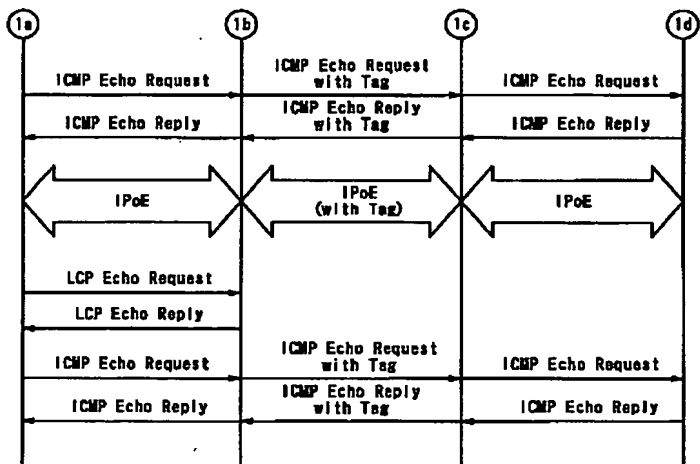
- A: プロバイダ側エッジL2SW: (ISP-Y接続ユーザが配下に存在する)
 B: プロバイダ側エッジL2SW: (ISP-Y接続ユーザが配下に存在しない)
 C: プロバイダ側エッジL2SW: (ISP-Yが接続されている)

【図32】



- A: プロバイダ側エッジL2 SW: (ISP-Y接続ユーザが配下に存在する)
- B: プロバイダ側エッジL2 SW: (ISP-Y接続ユーザが配下に存在しない)
- C: プロバイダ側エッジL2 SW: (ISP-Yが接続されている)

【図34】



【図35】

ポート	VLAN-ID
6	10
6	11
7	12

固定値として登録
(ただし、プロバイダはID
については変更する必要なし)

ポートVLAN-IDテーブル (プロバイダ側エッジL2 SW)

IP 7ドバイ	MAC 7ドバイ
x	X

For VLAN-ID=10

IP 7ドバイ	MAC 7ドバイ
y	Y

For VLAN-ID=11

IP 7ドバイ	MAC 7ドバイ
z	Z

For VLAN-ID=12

ARPリレーテーブル (プロバイダ側エッジL2 SW)

MAC7ドバイ	出力 ポート
A	1
X	5

For VLAN-ID=10

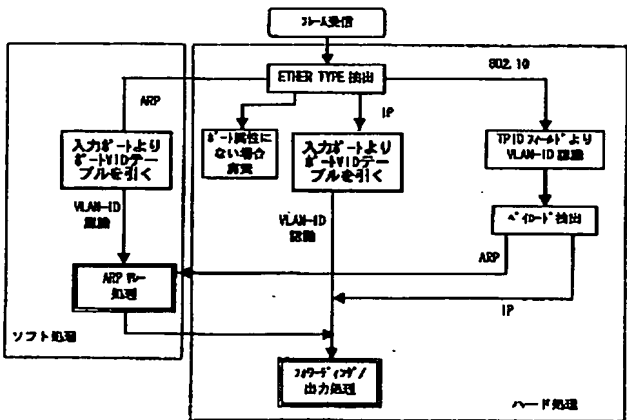
MAC7ドバイ	出力 ポート
B	2
D	4
Y	6

For VLAN-ID=11

MAC7ドバイ	出力 ポート
C	3
Z	7

For VLAN-ID=12

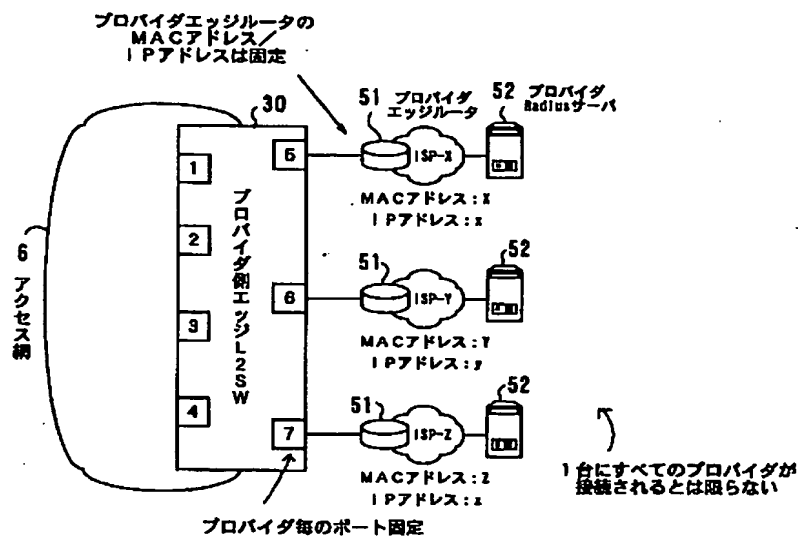
【図38】



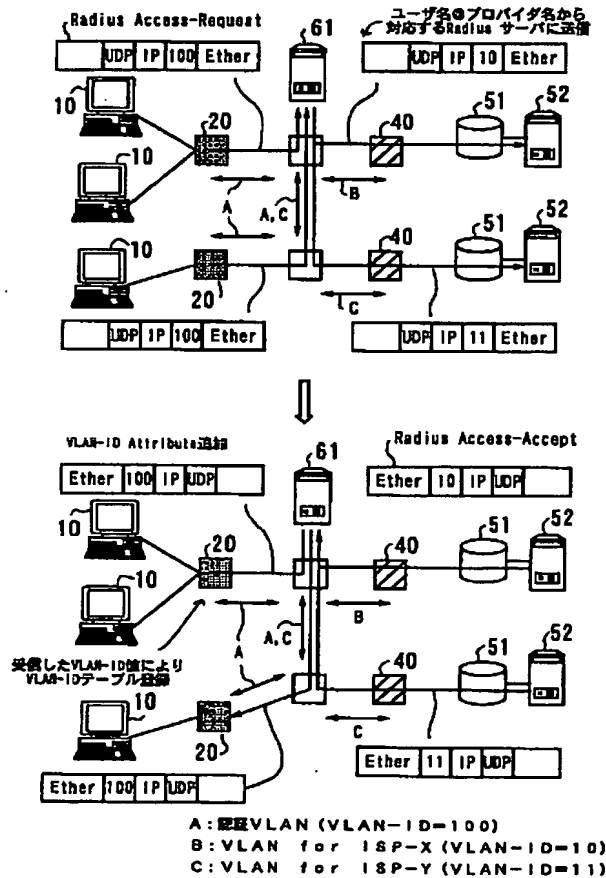
ポート	受信フレーム	ブロードキャスト フィルタリング	タグ挿入
1	IEEE802.1Q, GVRP, STP	OFF	With Tag
2	IEEE802.1Q, GVRP, STP	OFF	With Tag
3	IEEE802.1Q, GVRP, STP	OFF	With Tag
4	IEEE802.1Q, GVRP, STP	OFF	With Tag
5	IP, ARP	ON	UnTag
6	IP, ARP	ON	UnTag
7	IP, ARP	ON	UnTag

ポート属性テーブル (VLAN-ID毎に独立してもよい)

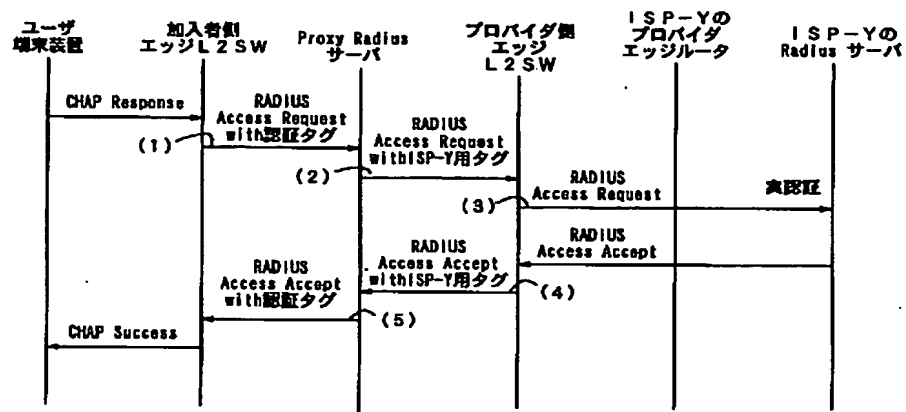
【図36】



【図39】

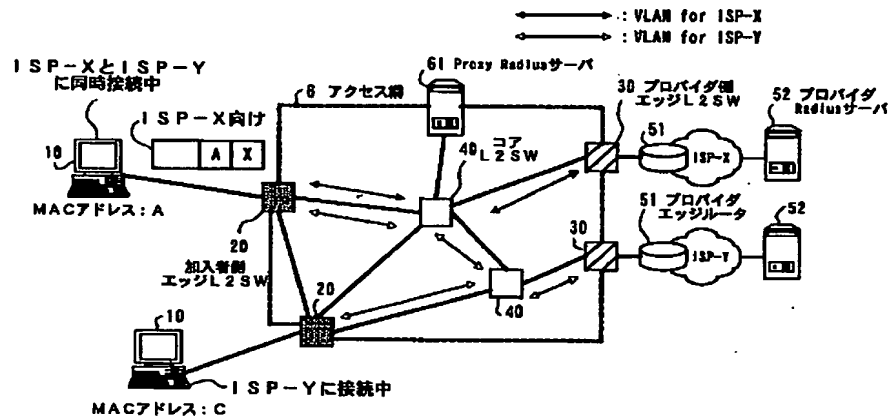


【図41】



- (1) 認証タグを付加してProxy Radiusサーバに送信
 (2) 接続先プロバイダを識別、対応するタグに付け替えて転送
 (3) タグ除去
 (4) 入力ポートよりISP-Y用タグを付加
 (5) ISP-Yに対応するタグID値を属性として追加して転送

【図43】



【図44】

MACアドレス	セッションID	VLAN-ID
A	0x1234	10
A	0x5678	11
	0x7777	
C	0x3869	11

送信元MACアドレスだけで
VLAN-IDテーブルを引くと複数
VLANにマッチしてしまう

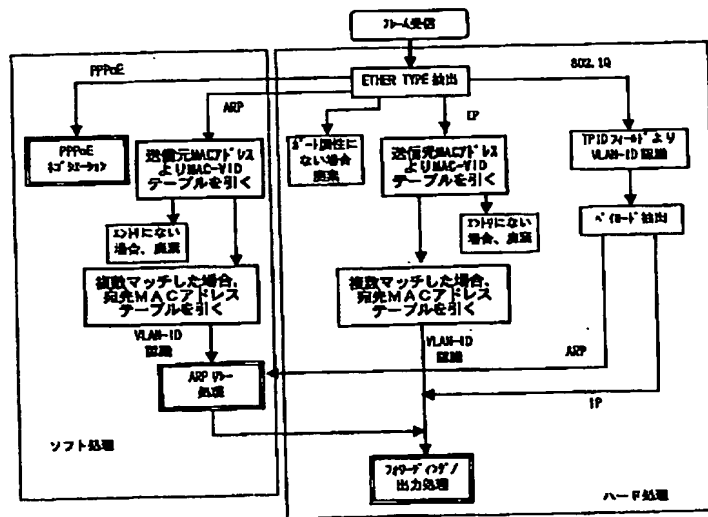
複数同時接続時のMAC-VLAN-IDテーブル

宛先MACアドレス	VLAN-ID
X	10
Y	11

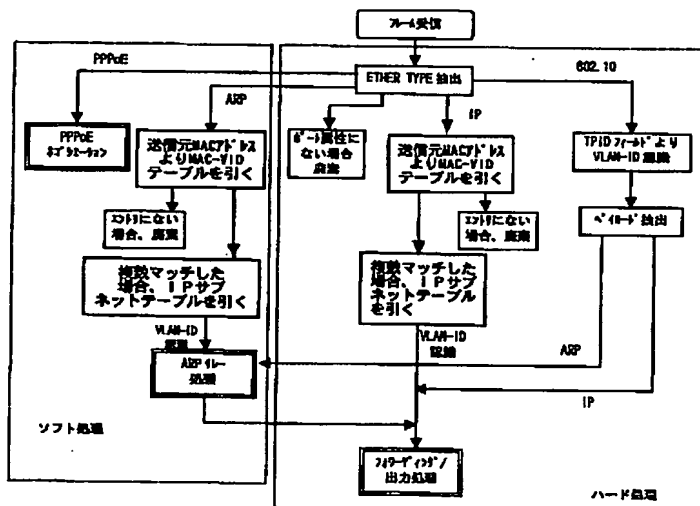
宛先MACアドレスにより
VLAN-ID=10と識別

宛先MACアドレステーブル
(ARPプライをもとに作成)

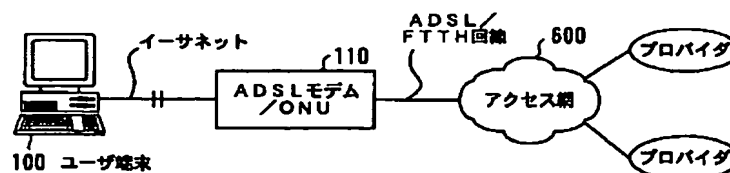
【図45】



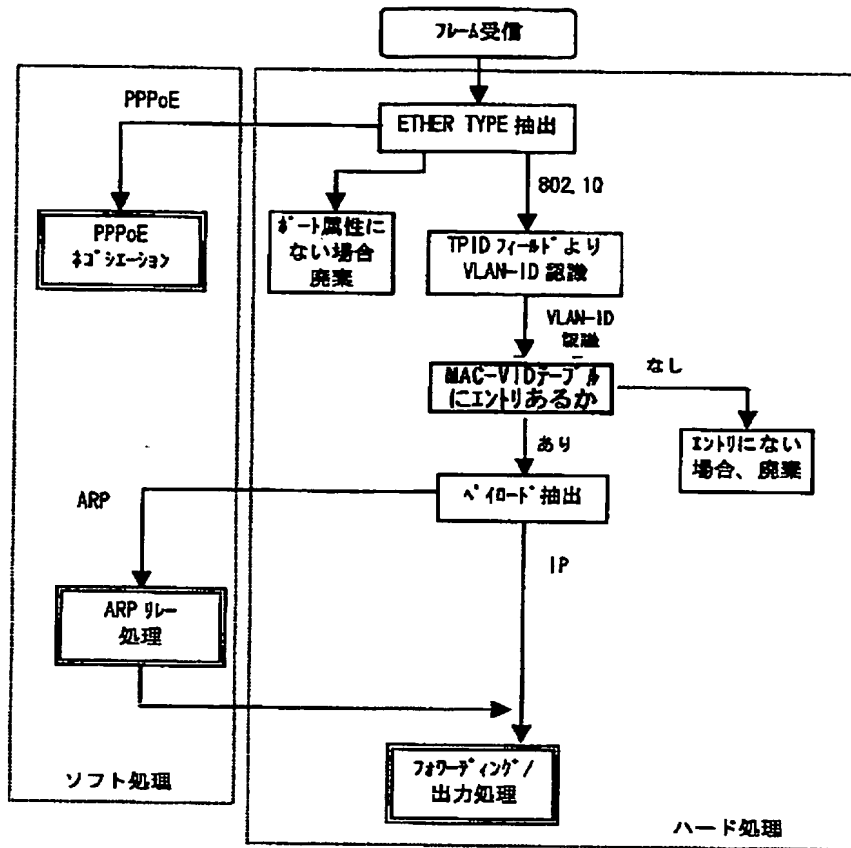
【図48】



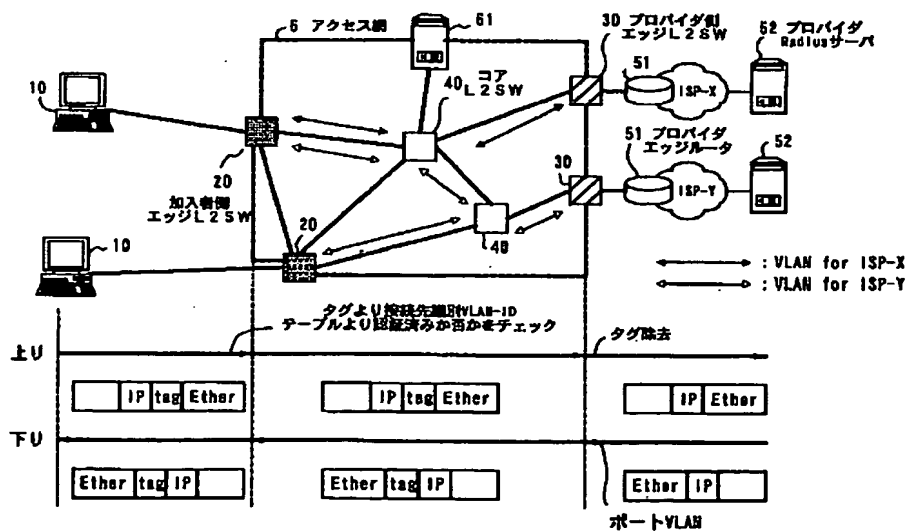
【図65】



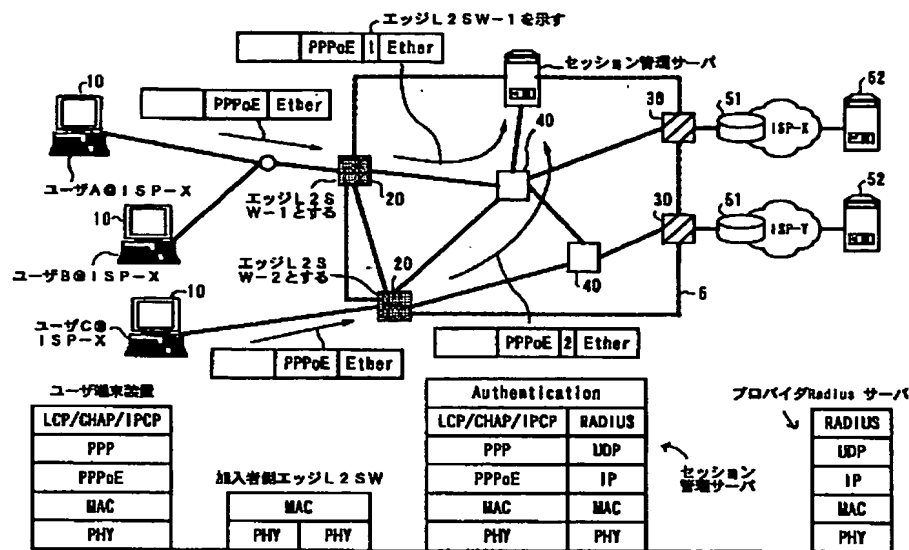
【図49】



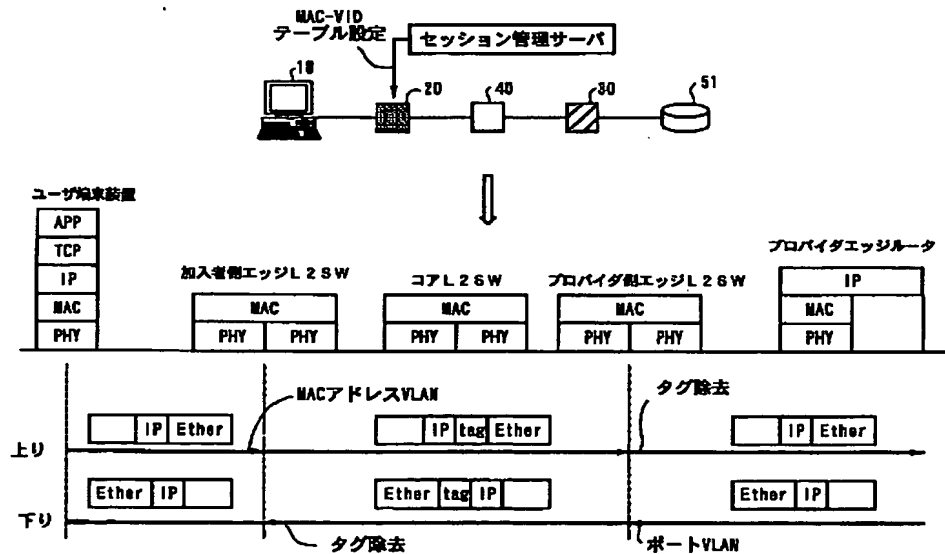
【図50】



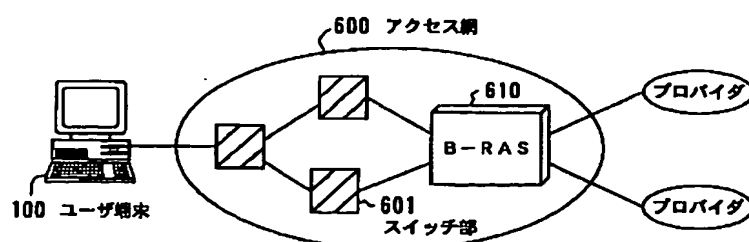
【図51】



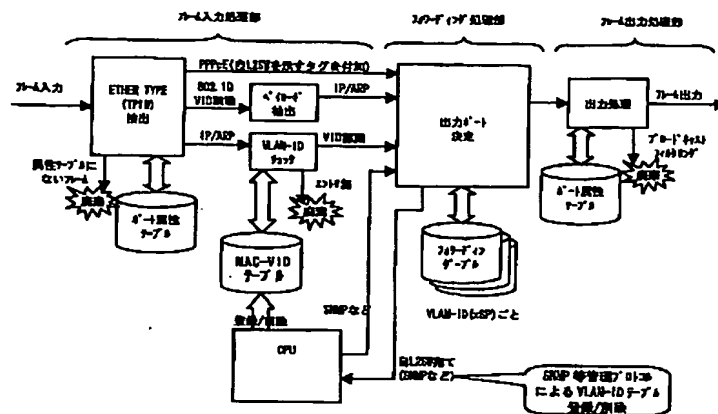
【図52】



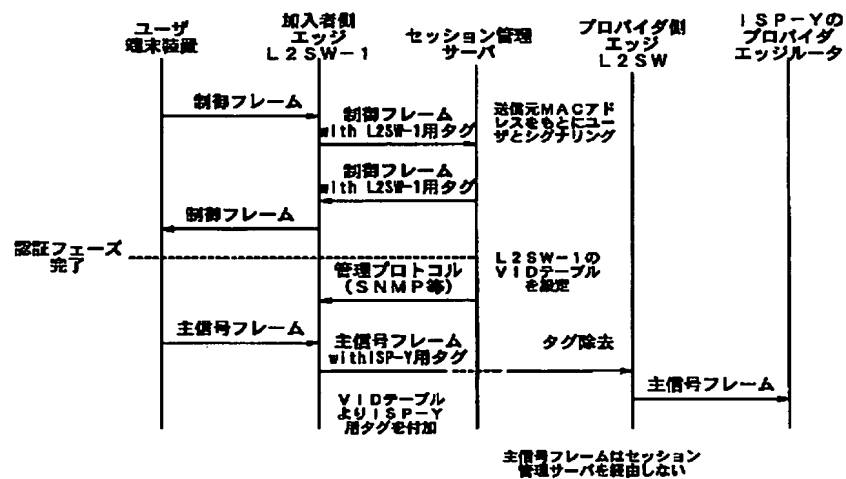
【図66】



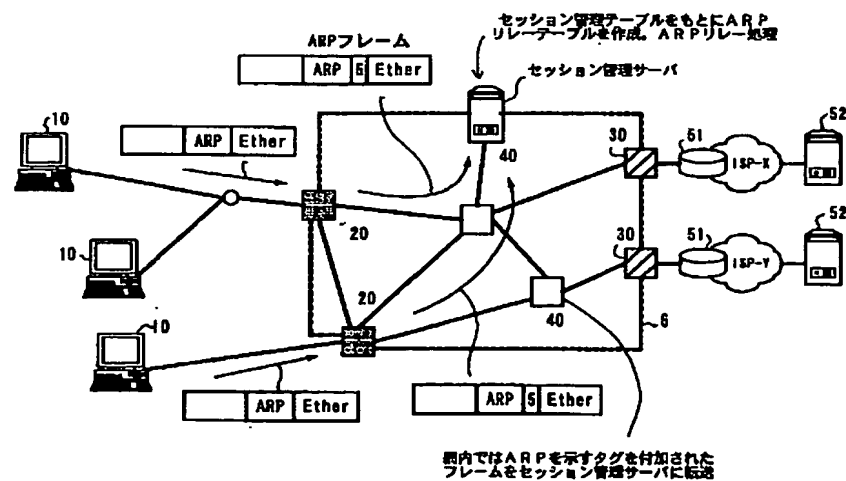
【図53】



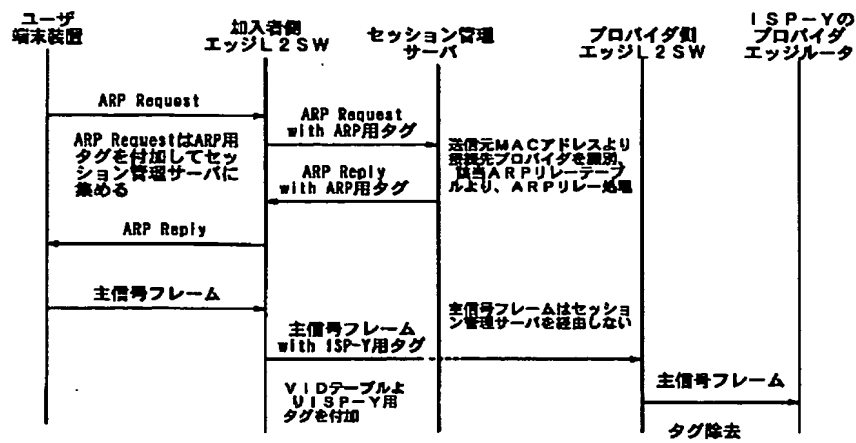
【図54】



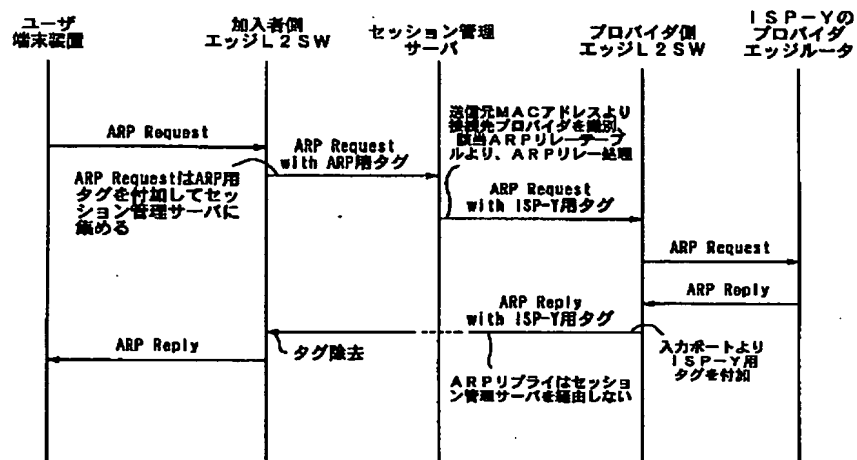
【図55】



【図56】

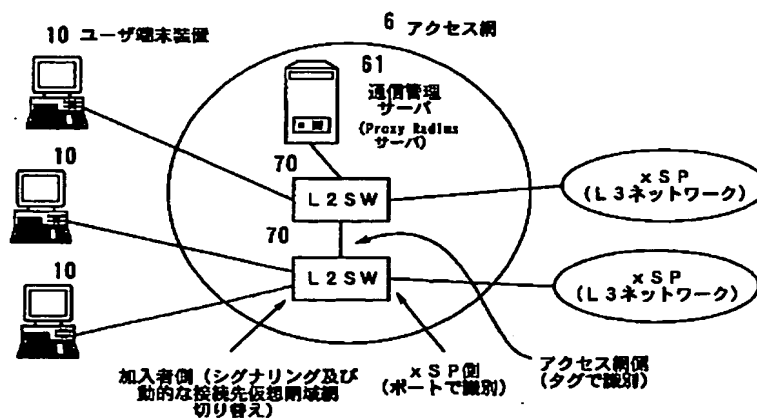


【図57】

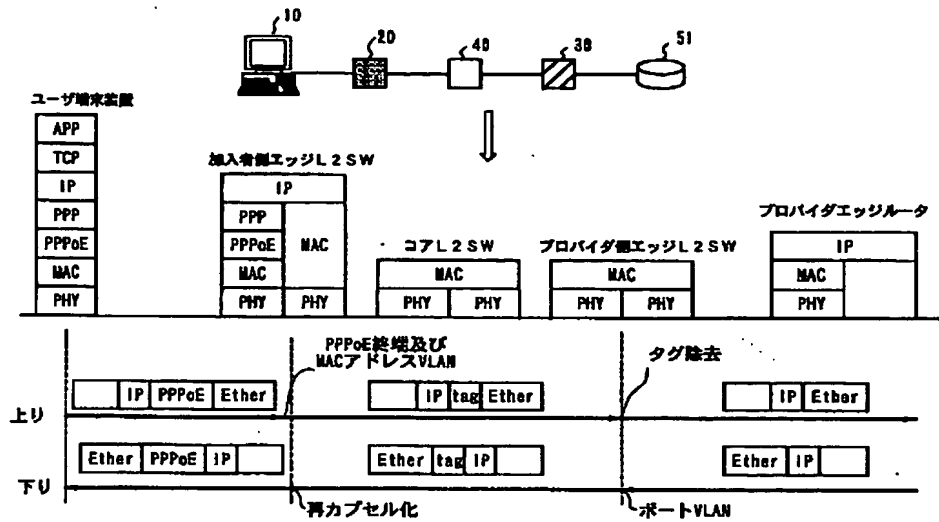


【図60】

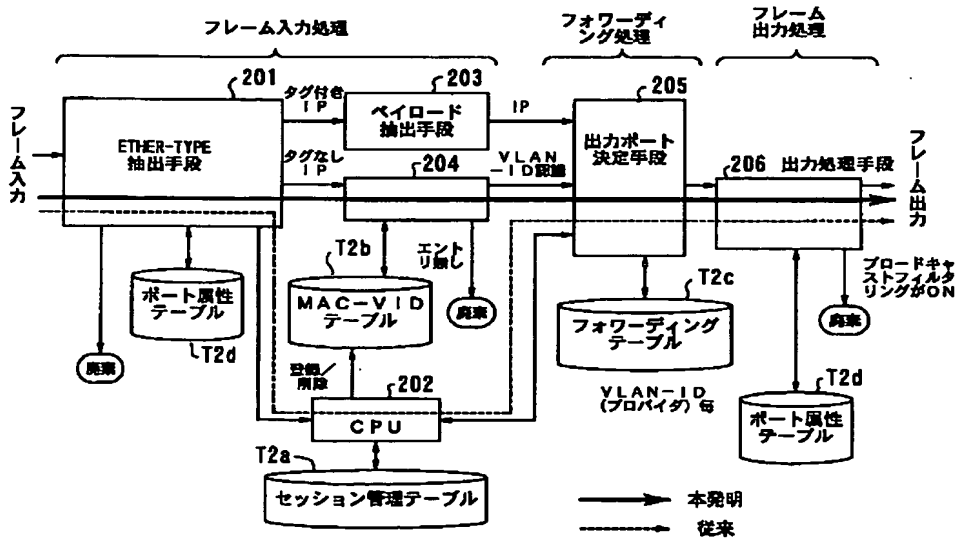
1a 通信システム



【図58】



【図59】



【図61】

追加パラメータ
↓

ポート属性テーブル (加入者側)

ポート番号	ポート属性	V I D	受信フレーム	ブロードキャストフィルタリング	タグ挿抜
1	user	—	PPPoE, IP, ARP	ON	UnTag
2	user	—	PPPoE, IP, ARP	ON	UnTag
3	user	—	PPPoE, IP, ARP	ON	UnTag
4	user	—	PPPoE, IP, ARP	ON	UnTag
5	core	—	IEEE802.1Q, GVRP, STP	OFF	With Tag
6	core	—	IEEE802.1Q, GVRP, STP	OFF	With Tag
7	core	—	IEEE802.1Q, GVRP, STP	OFF	With Tag
----	----	----	----	----	----

ポート属性値によってデフォルト値が自動設定

【図62】

追加パラメータ
↓

ポート属性テーブル (x S P側)

ポート番号	ポート属性	V I D	受信フレーム	ブロードキャストフィルタリング	タグ挿抜
1	core	—	IEEE802.1Q, GVRP, STP	OFF	With Tag
2	core	—	IEEE802.1Q, GVRP, STP	OFF	With Tag
3	core	—	IEEE802.1Q, GVRP, STP	OFF	With Tag
4	core	—	IEEE802.1Q, GVRP, STP	OFF	With Tag
5	xsp	10	IP, ARP	ON	UnTag
6	xsp	11	IP, ARP	ON	UnTag
7	xsp	12	IP, ARP	ON	UnTag
----	----	----	----	----	----

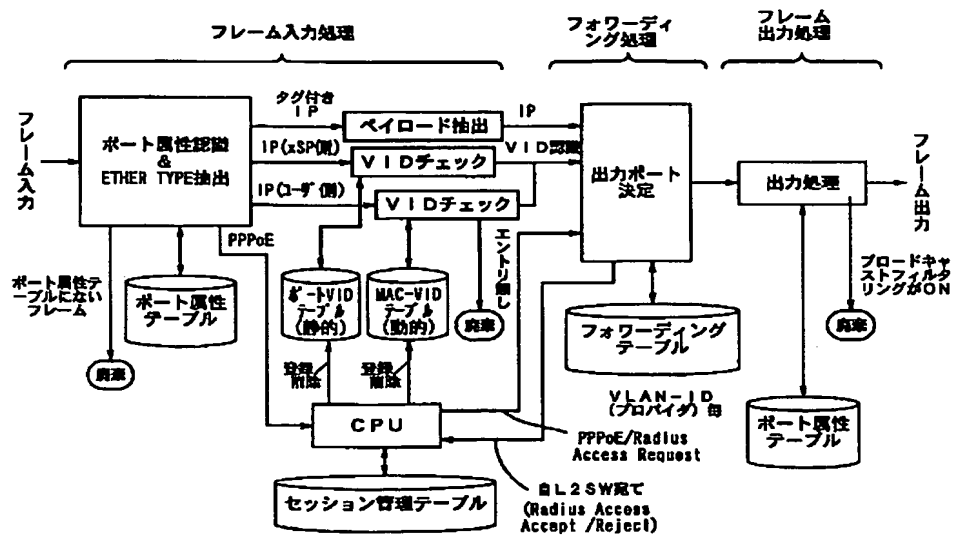
ポート属性値によってデフォルト値が自動設定

ポート番号	V I D
5	10
6	11
7	12
----	----

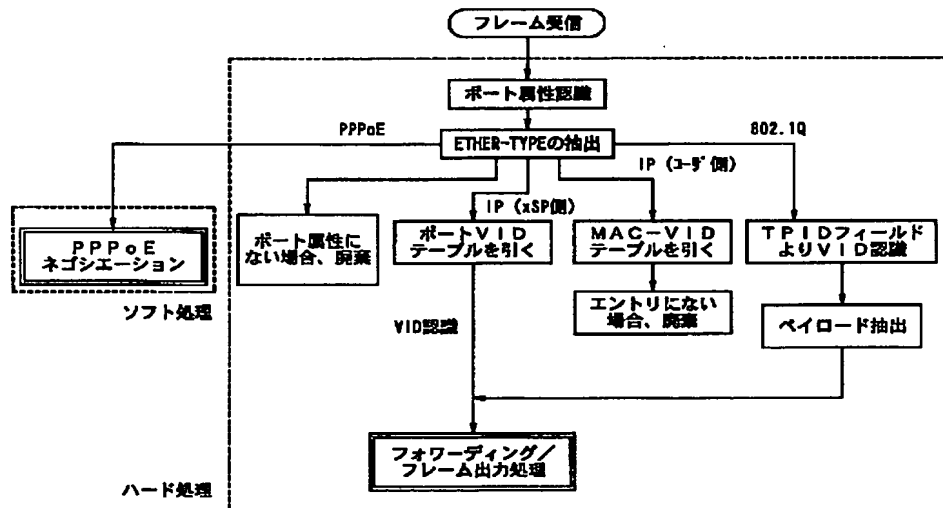
上記ユーザ設定値により登録

ポートV I Dテーブル

【図63】



【図64】



フロントページの続き

Fターム(参考) 5K030 HA08 HC01 HC13 HD08 HD09
 5K033 AA08 CB01 CB02 CB08 DA05
 EC03
 5K034 AA05 DD02 EE10 LL01

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER: _____**

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.